EAPB position on the EBA consultation on Draft Guidelines on internal governance (EBA-CP-2016-16)

Subject matter, scope and definitions

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

- **Clarification of non-binding nature of the Guidelines (GL):**

In the "Scope of application" section we suggest to make it clear that the word "should" has only the character of a recommendation and that deviations form the recommendations are permitted, especially taking the principle of proportionality into consideration.

- **Key function holder definition:**

We suggest keeping the number of people defined as key function holders as small as possible. This also applies for the "selection and suitability process" for key function holders (para. 19 (g)). In this context, we propose restricting this process to the heads of internal control functions and thus make a distinction from "other key function holders".

- **Mangement body definition:**

The definition of the management body in its management function seems inappropriate for certain governance structures as in some Members States the management function may not be formally represented on the Board of Directors. When there is no executive member on the board of directors (for instance in order to respect the proportion of independent members or other legal constraints) the distinction between supervisory function and management function is not applicable with the provided definitions. The definition could clarify that in the case of a company with a board of directors, the management function is performed by the executive members of the board (if any) and / or executive officers (see banking regulations of the Member State). Para. 32 of the draft GL should also take this into account and allow for a collegiality in the management function that could in some specific cases be limited to two people (CEO, Deputy CEO).

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?

- **Responsibilites of the management body:**

As mentioned in the answer to Q1 the draft GL are not appropriate for companies with board of directors with regard to certain responsibilities.

- **Notes on the relationship between the Internal Audit Function (IAF) and the Management Body (MB):**

The current draft GL are continuing a development according to which the IAF's role in reviewing an institution's compliance with its internal policies and procedures for the management body in its supervisory function (subsequently: MBSF) is extended. However, this development needs to be adapted for Member States with a dual board structure as the executive board bears full responsibility for the management of the company and exerts managerial authority over employees.

We therefore suggest the following detailed amendments:

- In the introductory section in para. 9 it should be clarified that it is up to the national regulator to assign tasks to the relevant body wherever the GL use the term "management body" without more detailed specification (see table on p. 19; this should be included in the final GL text as a seperate passage and should refer to the entire GL text and not just individual sections). Whereas the MBSF could be entitled with the right to ask questions or request reports by the heads of the IAF (under the prerequisite that the executive board is made aware of the exchanged information), there shouldn't be proactive IAF reporting obligations towards the MBSF. According to some national corporate governance frameworks, IAF management control instruments are the responsibility of the executive board which, in turn, bears full responsibility for management of the company and is accountable to the supervisory body. The IAF usually

reports to the executive board and from there the information is communicated to the supervisory body. Parallel lines of reporting from the heads of the IAF to the executive board and the supervisory body, however, would lead to potential conflicts of interests, particularly if the reporting obligation is combined with an "accountability" of the heads of the IAF to the MBSF as well as the MBSF having significant participation in personnel decisions. Split responsibilities and potential conflicts of interest would ultimately make it very difficult to carry out different tasks. At the same time, the executive board's ability to manage would be lost which would weaken the system of corporate governance in certain Member States at its core.

- The GL, p. 17-18, para. 23, stipulate that the body responsible for supervision, in this case the supervisory body, ensures inter alia the integrity of the financial information and reporting: "The management body in its supervisory function should also ensure the integrity of the financial information and reporting, and internal audit framework, including effective and sound risk management". This regulation seems to be in contrast to company law of several Member States since the management responsibility of the executive board is affected and the supervisory body, as the controlling body, is essentially unauthorised to undertake management measures. Measures which need to be taken to ensure the integrity of financial reporting should be viewed as management measures. We therefore recommend changing the wording of para. 23 so that the provision is aligned with the supervisory function of the supervisory body and the statutes of the corporation (e.g. submit recommendations or proposals to ensure the integrity of the financial information and reporting […]).

- On p. 17, para. 24 a. we suggest the following version (insertion underlined): "*The management body in its supervisory function should: a) have suitable members who do not perform any executive function in the institution and are collectively able to understand and oversee fully the risk strategy and risk appetite of the institution*;"

- P. 18, para. 24 g. and h.: As in para. 23, the word "ensure" is used. With reference to the above argument, we also recommend using an alternative wording here that considers the supervisory function of the supervisory body.

- P. 22, para. 46 b.: It should be clarified here that the executive board (Management Body in its Management Function, MBMF) supplies this information to the risk committee and the nomination committee of the supervisory body (MBSF) and not the heads of the IAF. It should also be clarified that only information relevant to the respective supervisory activity of the committees concerned, is supplied. It is not obvious why the nomination committee should be informed about risk limits, for instance.

- P. 29, para. 73, line 4: "and the internal audit function" should be removed.

- In accordance with p. 39, para. 122 of the GL, the head of the IAF should report directly to the supervisory body if his position is below the level of the executive board ("be directly accountable to the management body in its supervisory function."). This is in contradiction to the company law of some Member States in which "only" the supervision of the executive board and not the supervision of levels below the executive board, is incumbent on the supervisory body.

- P. 40, para. 124: Since the heads of the IAF can be also be positioned at the level of senior managers in accordance with the definition on p. 13 and in accordance with p. 29, para. 122, the second sentence should be reworded as follows: "*In any case, heads of internal audit functions ~~should – and, under Article 76(5) of Directive 2013/36/EU, the head of the risk management function~~ must not be removed without reasonable prior information of the management body in its supervisory function [on the reasons for the removal].*"

- P. 47, para. 168, lines 5 and 6: "in its supervisory function" should be removed.

In general, it should be noted that the notion of the executive function is not explained in detail. We therefore suggest incorporating a clearer definition.

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

In general, the GL appear to be clear regarding the role of the management body. However, the rules for the composition of committees and the accumulation of requirements can be problematic. A minimum of flexibility is necessary depending, for instance, on the composition of the boards (for example, when national law provides for a number of employee representatives within the board or specific requirements for companies with public ownership). We therefore have the following remarks/suggestions:

- The GL assume that the banks are able to influence the membership of the supervisory board and therefore have a certain discretion in terms of the people represented on the committee (in terms of adequate knowledge, skills, experience and diversity). In this regard, we think that this is not the case for all institutions. In certain cases, the supervisory body consists of representatives and the composition of the employee representation is determined by vote. In these cases, the bank itself has no right, of any kind, to participate in the membership of the supervisory body. This has an influence on all requirements that demand active control of the membership of the supervisory body.

- P. 21, para. 37: With the help of the GL, the lending banks should "*ensure*" that the committees of the supervisory body are not predominantly occupied by the same persons. However, we would like to point out that in most jurisdicitions the supervisory body is from a legal point of view relatively free to decide upon the membership of its committees. A corresponding "insurance" by the banks is therefore only possible by means of a statutory regulation which is associated with high cost and organisational complexity. Thus, we recommend an alternative wording in the GL (e.g. "[…] *it is suggested that committees are not composed mainly of the same group of members who form another committee*.")

- P. 21, para. 43: According to para. 43 of the GL, it is necessary that the skills, abilities and experiences are present among the members of the risk and nomination committees both individually and collectively. According to certain national laws, the risk committee (as with the other committees), however, is constituted from among the supervisory body which, due to its organisational sovereignty is in principle free to make decisions concerning the membership of the committees. With the stipulation for the individual aptitude of members of the nomination and risk committees, free decision making by the supervisory body over the membership of the committees is no longer possible. Such a restriction would need to be implemented into national law or by means of statutory changes. The latter is associated with high cost and organisational complexity which is why we re sceptic towards this requirement.

- P. 22, para. 44: The provision concerning the independence of the chair of the supervisory body committees can cause problems in certain cases. Due to the special business model of promotional banks that pursue public policy objectives and have public owners (central or regional governments or local authorities), the supervisory bodies of promotional banks often form sub-committees tasked with promotional issues, for example. Due to the public ownership a representative of the respective government or authority should chair these committees in order to ensure that the strategy and direction of the bank are in line with its public policy objectives. A reference to the "principle of proportionality" could be a potential solution for this issue.

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

- P. 28, para. 70: The requirements for an internal governance policy for the institutions are being considerably broadened. According to para. 70 sentence 1 "the management body [should] define, adopt and maintain a governance policy to implement a clear organisational and operational structure with well-defined, transparent and consistent lines of responsibility". The issues outlined in Annex 1 should be taken into consideration here. The control functions (risk controlling and compliance functions as well as internal auditing) must be comprehensively involved ("provide effective input") when preparing the internal governance policy. The compliance function is particularly emphasised ("should analyse how the policy affects the institution's compliance with legislation, regulations and internal policies"). In para. 70 sentence 3 and para. 73, the requirements of the supervisory body in terms of the supervision of the internal governance policy are considerably expanded. In fulfilling the requirements with respect to the listed issues, the risk controlling and compliance functions as well as internal auditing often overlap in the scope of their activity. The supervisory body is also already responsible for supervision of compliance with the requirements for proper business organisation. The requirement for a fixed written internal governance

policy amounts to pure formalism which ultimately only results in additional documentation for the institutions. We therefore suggest removing the explicit requirement for a written internal governance policy.

- P. 31, para. 85: We would like to point out that the code of conduct also applies for "external service providers" and that it is not clear how compliance can be precipitated, supervised and, if necessary, implemented. Further, it would be important to clarify who should be responsible for supervision of the compliance with the code of conduct, who should provide training and, also explanations of what the consequences of non-compliance might be.

- P. 35, para. 104-105: Competent auhorities should establish mechanisms for the reporting of breaches of supervisory requirements. There is already an option for employees to report directly to supervisors. Thus, we think that the current form of 'whistle blowing' should be considered as sufficient and that „encouragement“ to report breaches doesn't seem to be necessary.

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

- In general, we welcome the list of criteria which have to be taken into account when applying the principle of proportionality. Nonetheless, we think that additionally also the size of the workforce, the complexity of the legal structure, and the existence of a state guarantee or similar instruments for the institution‘s liablities should be added to that list.

- Further, we would like to highlight that the application of the principle of proportionality plays a crucial role for promotional banks. Promotional banks are especially characterized by their public ownership, the pursuit of public policy objectives and their low-risk business model. All these aspects need to be duly taken into account when applying these GL.

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

- P. 38, para. 113: The differentiation between the three 'lines of defence' seems to be a bit unclear. According to the GL the business line is the first line of defence, risk management and compliance the second and the internal audit function the third. This should be made clearer in para. 113 since "internal audit function" is used collectively, as well.

- P. 38, para. 113 states that the institutions should develop an internal control framework and a risk management framework. According to our understanding, this does not mean an all-encompassing document for each of the issues of internal audit and risk management but rather, respective basic framework documents coupled with additional operational substantiations (e.g. in the form of operating instructions) for each basic framework document (an internal audit framework and a risk management framework). We request clarification that this means basic framework documents with additional operational substantiations for each.

- P. 39, para. 116: In this context, it should be clarified that this is understood as a framework and not as instructions for the daily business.

- para. 123 and 150: The requirement that the head of internal auditing/the risk management function, reports directly to the supervisory body isn't in line with the corporate law of several Member States. Thus, an implementation of this rule would require legislative amendments or a change of statutory provisions of the affected banks.

- P. 41, para. 130: A "holistic institution wide risk management framework" is being discussed as a part of the overall internal audit framework. In this context, we woudl like to request clarification on the relationship between the internal audit framework and the risk management framework. For instance, it should be clarified that the focus of a risk management framework is on the risk management function (and not on all internal audit functions, including the compliance function and the internal control function). In our opinion, an overview of all of the control functions would be part of the overall internal control framework.

- P. 43, para. 140: As an independent supervisory function, internal auditing fulfils an important management function. In a dual governance structure, it seems appropriate that internal auditing - while preserving the independence and accessibility offered by the supervisory body - should be associated with management.

- P. 43, para. 143: It is noted that there are requirements for the new products approval policy (NPAP) and material changes to operating processes and systems. According to sentence 1, the NPAP should be carried out through "the development of new markets, products and services and significant changes to existing ones". According to sentence 2, an institution must also have "appropriate change policies for material changes to processes and systems". However, in para. 144 et seq., the two statements are not always distinguished consistently, so it is unclear whether the requirements of each paragraph refer exclusively to the NPAP or to the NPAP and the material changes to processes and systems. Only para. 146 and para. 147 refer explicitly to the NPAP. Para. 144 and para. 145 only generally refer to policies. Para. 148, on the other hand, talks of "significant changes to existing products, processes and systems", in which it is unclear whether "material changes to processes and systems", in the sense of para. 143 sentence 2, is meant in addition to the NPAP (significant changes to existing products). We therefore suggest clearly separating the requirements of the NPAP and the material changes of processes and systems in the GL. The compliance and risk management functions should be incorporated into both the NPAP and into the material changes for operating processes and systems. This corresponds with the applicable requirements that already exist. Aside from the two control functions, all of the organisational units that are subsequently integrated into the work processes, as well as internal auditing, are already regularly a part of the NPAP in practice. Para. 145 is new and requires an institution to have "specific procedures for assessing compliance with these policies" for the NPAP (and, if necessary, for material changes to processes and systems - see paragraph 1). "This should include a systematic prior assessment and approval by the compliance function, including a written opinion from the head of compliance". Furthermore, in para. 181 of chapter 15 of the EBA GL, it says "the compliance function should also verify, that new products and new procedures comply with the current legal framework and where appropriate, any known forthcoming changes to legislation, regulations and supervisory requirements". The requirement for the compliance function in the NPAP is described appropriately and sufficiently in para. 181 of chapter 15. The additional "specific procedures for assessing compliance" are therefore unnecessary. Furthermore, a "written opinion from the head of compliance" in the sense of a final release of the NPAP by the compliance function is not considered expedient. This applies particularly if para. 145, beyond the NPAP, is supposed to refer to "material changes to processes and systems". There is no overall responsibility of the compliance function for the NPAP. Instead, the contribution of the compliance function to the NPAP is more of a - if not more important - component of the NPAP. We therefore suggest this passage be removed.

- P. 44, para. 144 and 145: The suggested requirements of the compliance function would mean a strong change of the "three lines of defence model". Under the new requirements, the compliance functions are to assume tasks which are currently being completed either by the first line of defence - i.e. the specialist areas - or, in particular, by the third line of defence, internal auditing, through their ongoing audits. This is resulting in considerable overlaps and inefficient duplicate working, especially in auditing. Usually, the compliance function is tasked with analysing the impact of significant planned changes on control procedures and the control intensity and not with the compliance and regular review of important changes and guidelines. Internal auditing is responsible for this.

- P. 44, para. 148: In light of the multitude of requirements for scenario analysis, a requirement of "under a variety of scenarios" would result in an unreasonable additional burden with limited additional benefits.

- P. 44, para. 149 et seq.: The risk management function was called the "risk control function" in the current GL. It is unclear whether this is simply a formal renaming or if it is associated with material changes. The reasons for the renaming should therefore be given in the explanations on the new GL and it should be made clear whether new meaning is associated with this new naming i.e. whether the new term represents something more.

- P. 45, para. 154: A group wide, extensive look at all of the risks ("holistic view on all risks") related to compliance with the risk strategy is needed here. This does not seem to be expedient.

- P. 45, para. 154, 161, 164: Inter alia, the term "all risks" is used in these sections. A clarification would be helpful here on whether all the risks should be focused on or just those categorized as significant. In para. 161 (p. 46), in particular, it should be pointed out that not all risks - as required - can be "measured" (especially in the case of non-financial risks). Based on the principle of proportionality, this requirement should be limited to "significant risks".

- P. 47, para. 170: This regulation represents an extension of the risk management function. Currently this is the responsibility of compliance.

- P. 47, para. 172: We request clarification on whether the head of risk management function is equivalent to the chief risk officer (CRO) and whether this should be positioned at the CEO levels exclusively with this purpose in the case of significant institutions. Furthermore, we request clarification on whether there is a strict separation of tasks only if the head of the risk management function is positioned at a sub-management level.

- P. 49, para. 186: We suggest making the following addition: “The IAF should independently review the compliance of all activities and units of an institution including outsourced activities with institutions’ policies and procedures and this should ensure that each material entity within the group falls within the scope of the IAF." An extension to all participating interests would result in the consideration of a multitude of insignificant participating interests. This is not risk oriented in terms of MaRisk and is inefficient on top of that.

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

- The guidelines are quite clear regarding transparency of the organization of the institution. However, it could be inappropriate to publish an overview of material outsourcing of activities, process and systems (with respect to confidentiality of the business organization). Further, we suggest adding to the requirement for disclosure of evidence that the disclosure requirement has been sufficiently met via electronic publication (e.g. on the internal intranet).

Remarks on Annex 1

It would make sense to clarify that 7c (weaknesses identified by each internal audit function and measures taken to address them) and 7d (recommendations made by the internal audit function and measures taken to implement them) refer to overall handling of weaknesses identified by the control functions and their management measures (allocation of responsibilities) - and not to each individual case.