German Banking Industry Committee

Die Deutsche Kreditwirtschaft

# Comments

## EBA Draft Guidelines on internal governance

Register of Interest Representatives
Identification number in the register: 52646912360-95


Contact:

Thomas Lorenz
Director
Telephone: +49 30 1663 3190
Email: thomas.lorenz@bdb.de

Torsten Jäger
Division Manager
Telephone: +49 30 1663 2160
torsten.jaeger@bdb.de


Berlin, 27 January 2017

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. Collectively, they represent approximately 1,700 banks.


Coordinator:
Association of German Banks
Burgstraße 28 | 10178 Berlin | Germany
Telephone: +49 30 1663-0
Telefax: +49 30 1663-1399
www.die-deutsche-kreditwirtschaft.de

## Comments on the EBA Draft Guidelines on internal governance

**Q1: Are the guidelines regarding the subject matter, scope, definitions and implementation appropriate and sufficiently clear? [Paragraphs 1-15]**

**Paragraphs 8-12**
We suggest making clear that the word "*should*" in the guidelines always only has recommendatory character and that, when the guidelines are transposed at national level, it allows derogations taking due account particularly of the principle of proportionality and national company law.

**Paragraph 13**

- *"Significant institutions"*: the competent authority is to be able to determine, where appropriate, other institutions as significant in addition to systemically important institutions. How these are to be defined remains unclear, however. As the guidelines on identifying systemically important institutions already take into account criteria such as an institution's size, the complexity of its business, etc., a separate definition for the purposes of the guidelines on internal governance is unnecessary, in our view. We believe that the definitions should be based on systemic importance and that "*significant institutions*" should be replaced throughout the guidelines by "*systemically important institutions*".

- "*Key function holders*": We would welcome clarification on what is meant by "*other key function holders*". It is not clear from the definition which persons it covers as a whole.

- "*Chief Financial Officer*": It would be clearer if the word "risks" were removed from the definition of "*Chief Financial Officer*", as this implies the management of financial risks such as credit or market risks.

- "*Conflicts of interest*": We would appreciate clarification as to why the definition of "*conflicts of interest*" appears to exclude internal conflicts (i.e. only conflicts including a personal interest within the current definition).

**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? [paragraphs 16-33]**

Yes. The present draft guidelines continue a trend whereby internal control functions are increasingly being used as a means of corporate oversight by the management body in its supervisory function (MBSF). This trend needs, however, to be reconciled with the two-tier corporate governance structure in Germany, comprising a management board (*Vorstand*) and supervisory board (*Aufsichtsrat*), in which the management board has overall responsibility for managing the company and exercises authority over employees.

We therefore suggest the following modifications:

- Paragraph 9 should expressly make clear that, when transposing the guidelines on internal governance, it is up to the national regulator to identify the right body under the relevant national company law regime wherever the guidelines use the term "*management body*" without specifying it any further (see also box on page 19f. – should be contained in the final text as a

passage in its own right and refer to the guidelines as a whole and not only to some sections thereof).

- It should also be made clear in paragraph 9 that if it is not specified whether the management body in its management function or in its supervisory function is meant, the management body in its management function is meant. Otherwise there is, in our view, the danger of the management body in its supervisory function being overburdened and of failure to achieve the actual objective of the guidelines, namely strengthening internal governance as part of corporate governance.
- Paragraph 23 of the guidelines says that the "*The management body in its supervisory function should also ensure the integrity of the financial information and reporting, and internal control framework, including effective and sound risk management*". This requirement breaches German stock corporation law: Section 91 of the German Stock Corporation Act (Aktiengesetz) requires the management board to take suitable measures, particularly setting up a monitoring system, so that developments threatening the continued operation of the company are detected at an early stage. The requirement to ensure this addressed to the supervisory body touches on the management body's responsibility to manage a company. The supervisory body, as an oversight body, is not in principle authorised to take management measures. Section 111 (4) of the German Stock Corporation Act states that "*management measures cannot be delegated to the supervisory board*". The measures that need to be taken to "*ensure the integrity of financial information and reporting and internal control framework, including effective and sound risk management*" are deemed to be management measures. Furthermore, under German banking supervisory law the management board is responsible for ensuring the institution's proper business organisation, which should also comprise appropriate and effective risk management (section 25a (1) of the German Banking Act (*Kreditwesengesetz*). Responsibility for the proper business organisation includes adopting appropriate arrangements by means of which the financial situation of the institution can be determined sufficiently accurately at all times (Section 25a (1) no. 6 of the German Banking Act). We therefore recommend amending the wording of paragraph 23 so that it also takes due account of the German legal requirements, particularly with regard to the oversight function performed by the supervisory body under German stock corporation law and the constitution of the German stock corporation (*Aktiengesellschaft*) (e.g. "*submit recommendations or proposals to ensure the integrity of the financial information and reporting, […]* ).
- We recommend wording paragraph 24 a) as follows (additional worded 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 <u>collectively</u> able to fully understand and oversee the risk strategy and the risk appetite of the institution;*".
- Paragraph 24 g) and h): Like under paragraph 23 above, the verb "*ensure*" is again used. With reference to the above line of argument on paragraph 23, we recommend adopting an alternative wording in this case as well to take due account of the supervisory body's oversight function.
- With regard to paragraph 24 g), we should like to draw attention to the conflict in that the heads of internal control functions are bound to the instructions of the management of an institution and should not bypass it to inform the supervisory board. Paragraph 24 should therefore be adapted to the structures defined under company law or deleted. In Germany, reporting by, for example, the internal audit function (IAF) to the supervisory body is regulated in such a way that it can be done via the management provided that that this does cause any significant delay in such reporting to the supervisory body and the content of reporting is identical.

**Comments on the EBA Draft Guidelines on internal governance**

- Paragraph 29: The wording "*should constructively participate in the discussions*" should be revised, as supervisory board members do not participate in management board meetings in the context of a two-tier system .

Whilst rights with regard to questions and reports between the management body in its supervisory function and the heads of internal control functions are acceptable on condition that the management body is always informed about the information exchanged, no requirement for internal control functions to report pro-actively direct to the MBSF should be set. Under the German corporate governance regime, internal control functions are a means of governance by the management body, which carries overall responsibility for managing the company and is accountable to the supervisory body. Reporting lines run from internal control functions to the management body and from there to the supervisory body. Parallel reporting lines from the heads of internal control functions to the management body AND the supervisory body would lead to split loyalties, particularly if they are combined with accountability by the heads of internal control functions to the MBSF and active involvement of the MBSF in human resources decisions in this area. Split responsibilities and loyalties will ultimately mean that no responsibility can be exercised in full. At the same time, the controllability of the management body would be lost, weakening the German system of corporate governance at its very core.

We therefore specifically recommend further modifications:

- Paragraph 46 b): It should be made clear here that the management body in its management function (MBMF) delivers this information to the MBSF's risk committee and nomination committees, and not the heads of internal control functions. It should also be made clear that information is only delivered for the purposes of each committee's oversight mandate. It is not clear why, for example, the nomination committee should be informed about risk limits.
- Paragraph 73, line 4: The wording "*and the internal audit function*" should be deleted.
- Paragraph 122: The head of the IAF, if positioned below management body level, is to be "*directly accountable to the management body in its supervisory function*". This is at odds with German stock corporation law, according to which the general view is that the supervisory body is responsibly "only" for overseeing the management body and not for overseeing the levels below the management body (see, for example, Habersack in MünchKomm/AktG, 4th edition, 2014, § 111, paragraph 25).
- Paragraph 124: As the heads of internal control functions as defined on page 13 and in paragraph 122 on page 39 may also be sited at division management level, the second sentence should be reworded as follows: "*In any case, the heads of internal control 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 ~~approval~~ information of the management body in its supervisory function [on the reasons for the removal]*."
- Paragraph 168, lines 5/6: The wording "*in its supervisory function*" should be deleted.

In a general context, it should be noted that "*executive function*" is not explained any further. We therefore recommend including a clear-cut definition.

**Paragraph 19 j)**
In our view, the requirement to establish a code of conduct, as also called for in paragraph 85, does not make sense for all institutions. Instead, it should only apply where it delivers real added value for an institution. Particularly in the case of very small, non-complex institutions where management and staff

usually conduct an intensive dialogue, a code of conduct is likely to merely impose an administrative burden without improving the risk situation. For this reason, the need to establish a code of conduct and its content should be geared to the nature, size and complexity of an institution's business.

**Paragraph 20**
The term "*communications*" should be explained and narrowed in scope. We assume that it means external communications (particularly investor relations, business reporting).

**Paragraph 33**
Paragraph 33 should differentiate between material developments threatening the institution as a whole, where there should be no undue delays, and other information where time is not of the essence.

**Q3: Are the guidelines in Title I regarding the role of the management body appropriate and sufficiently clear? [paragraphs 34-69]**

In the guidelines it is assumed that banks can influence the composition of the supervisory board and its committees and thus have a say in who is appointed to both (in terms of adequate knowledge, skills, experience and diversity). May we point out in this respect that not all institutions do have such capability. In some cases, for example in public banks, the majority of the supervisory body is elected by the local parliament or made up by representatives of the municipal trustee, meaning that the bank itself has no say whatsoever in the composition of the supervisory body. This makes the implementation of requirements calling for pro-active control of the composition of the supervisory body impossible in principle. In other cases, the members of the supervisory board are always elected by the shareholders, so that the bank has no say here either in the composition of the supervisory board. In Germany, there are, in addition, the rules on co-determination in the corporate sector, which – irrespective of the number of employees – may lead to part of the supervisory board being composed of elected employee representatives. As the current members of the supervisory body may not fulfil the new supervisory requirements, the time scope of application of these requirements should be confined to future members of the supervisory body.

**Paragraphs 34-41**
It should be clarified that any decision to set up specialised committees is at the discretion of the respective board and there is no requirement for such committees to be made up exclusively of non-executive directors. The audit committee should be included as a required committee for significant institutions as per Statutory Audit Directive 2014/56/EU.

**Paragraph 34**
According to the draft guidelines, the risk and nomination committees are to advise the supervisory body and prepare its decisions. If this is supposed to mean that committees are generally not allowed to make any decisions of their own, we expressly request an amendment. The supervisory body can be supported not only by way of purely preparatory acts but, in principle, also by means of decisions.
A decision made by the competent committee based on authorisation conferred by law and a company's constitution is therefore deemed to be a decision of the supervisory body. The envisaged constraint would unlawfully restrict the right accorded to the supervisory board of a German stock corporation under Section 107 (3) of the German Stock Corporation Act to delegate certain functions and decision-making powers to committees. The supervisory board of a German stock corporation, enjoying organisational sovereignty, is free to decide whether and, if so, to what extent – within the limits set by the German Stock Corporation Act – decision-making powers are delegated to the committees it sets up. In particular,

the existence of decision-making statutory nomination committees (which are required by a company's constitution) should not be called into question.

As delegation of certain decisions to a nomination committee is a long-standing, tried and tested practice, we call for retention of this decision-making power. The passage in the draft guidelines reading "*and to prepare the decisions to be taken by this body*" should therefore be deleted. It should at least be made clear that if committees provided for in a company's constitution are established (voluntarily) they should continue to be allowed to make decisions.

**Paragraph 37**
According to the draft guidelines, committees should not be composed mostly of the same group of members. This de facto ban on having committees composed of the same group of members is opposed to all practical considerations. Particularly where remuneration and nomination committees are concerned, there are often overlapping issues. The same goes for audit and risk committees. A flow of information and proper performance of supervisory body functions, also as regards sufficient time commitment for the performance of such functions, can only be ensured if composition of committees by the same group of members is allowed. The final sentence of paragraph 37 should therefore be reworded as follows: "*However, taking into account the size of the management body and the number of independent members of the management body in its supervisory function, institutions should ensure that not all committees are ~~not~~ being composed exclusively ~~mostly~~ of the same group of members ~~which form another committee~~.*"

In this context, it should also be borne in mind that at institutions with 'smaller' bodies (fewer than 10 persons) the establishment of committees would no longer be possible if there were to be a complete ban on such committees being composed of the same group of members. The relevant passage (final sentence of paragraph 37) should therefore be deleted.

**Paragraph 39**
It would be useful to recognise the different roles of the supervisory function within single and two-tier structures, specifically to provide guidance on how board committees could impact the management function in a two-tier structure, where there is no direct relationship as in a single-tier structure [see in this context comments on paragraph 47 (a) and 8 (d)]

**Paragraph 43**
Whereas under German supervisory law (Section 25d (2) of the German Banking Act [*Kreditwesengestz]*) the supervisory board as a whole is required to have the necessary knowledge, skills and experience, paragraph 43 of the draft guidelines says that members of the risk, nomination and audit committees, if any, and where required, should have such knowledge, skills and experience both individually and collectively. This would be particularly challenging for a two-tier system that has a very different set of individuals performing the supervisory function. On top of this, under German stock corporation law the risk committee (like the other committees) must be constituted from the midst of the supervisory body, whose organisational sovereignty allows it to freely decide on the composition of the committees as it sees fit. The requirement for the members of the nomination, risk and audit committees to be appropriately qualified individually means that the supervisory body is no longer free to decide on the composition of each committee.

## Comments on the EBA Draft Guidelines on internal governance

**Paragraphs 37, 42 and 44**
An appropriate number of independent supervisory board members is proposed. In our view, it should be made clear that this requirement only applies if the supervisory body is obligated to establish committees (risk, nomination or risk committee).

Furthermore, it is not clear what "*independent members*" actually means here. Does it mean that a member does not at the same time perform management functions within the same institution, or is the term to be understood along the lines of "*independence of mind*" as referred to in the current EBA consultation paper entitled *Draft Guidelines on the assessment of the suitability of members of the management body*? Clarification on this point is required, e.g. by using the same term as in the aforementioned EBA consultation paper. If the independence requirement goes beyond "*independence of mind*", this would cause problems for cooperative banks, for example, since the German Cooperatives Act (*Genossenschaftsgesetz*) stipulates that every supervisory board member usually has to be a member of the cooperative as well.

**Paragraph 42**
Under section 18, paragraph 123 of the EBA consultation paper *Joint EBA and ESMA Guidelines on the guidelines on the assessment of the members of the management body and key function holders*, the requirements relating to independence are put in very broad terms. These requirements rule out all the staff of companies that belong to the same consolidated group. The result is that, for example, in the case of a credit institution that is a wholly-owned subsidiary of a mixed holding company or industrial enterprise the risk committee would have to be made up predominantly of persons that are not members of the group. Particularly in the case of parent/subsidiary structures in mixed groups, it is, however, important that the representatives of the parent company monitor the risks effectively and can also limit these by way of arrangements giving right of approval to the supervisory board, as the credit institution's parent company would also be directly affected by risks not identified and limited by third parties. This task is performed mainly by the risk committee, which deals professionally with the risk situation, risk strategy, etc. The rule here should be that there is no separation of liability and control. The company that is liable should retain effective control of risks. Otherwise this may impair the ability of the management board of the non-supervised parent industrial enterprise operated in the form of a stock corporation (*Aktiengesellschaft*) to effectively carry out its duties in accordance with Section 91 (2) of the German Stock Corporation Act (*Aktiengesetz*). These consist in taking suitable measures so that developments threatening the continued operation of the company are detected at an early stage (cf. Section 93 (2) of the German Stock Corporation Act). In addition, assessing the risk profile and risk situation of captive finance companies calls for special knowledge of the business model and internal operations that outside persons usually do not have. We therefore request deletion of this paragraph or at least the inclusion of an 'opening clause' for the above-mentioned cases of credit institutions within mixed groups, stating that the majority of the members of the risk committee do not have to be independent.

**Paragraph 44**
The requirement in paragraph 44 for the chair of supervisory body committees to be independent is inappropriate in such absolute terms. Because of the special business model operated by a promotional bank with a public mandate, promotional banks' supervisory bodies usually set up sub-committees dealing with promotional issues, for example. These should be headed by the representative of a 'promotional ministry' and thus, by definition, by a 'non-independent person'. In addition, performance of some of the key functions of the supervisory body is inextricably linked to the 'promotional bank with a public mandate' business model in order to ensure that the strategy and focus of the bank are in line with the public mandate.

Furthermore, the requirement in paragraph 44 would mean that, for example, the Chief Financial Officer in an industrial enterprise that is the parent company of a credit institution would no longer be able to chair the risk committee or audit committee. Particularly in mixed groups, it is important that such oversight functions can also be delegated to persons who are typically entrusted with such functions within the group in order to ensure that the interests of shareholders, particularly asset protection, are duly taken into account (see in this context our remarks on paragraph 42).

A solution here would be a reference to the proportionality principle, particularly with regard to the business model.

**Paragraph 46**

- The requirement under point (a) for all members of the risk and nomination committees to have "*access to all relevant information and data …"* is, in our view, neither permissible nor necessary. Direct access to IT systems, hard drives, etc. is already ruled out by data protection and information security regulations. A definition is also difficult here: which data is "*relevant*"? What degree of detail is required? This point should, in our view, be deleted. Point b already lists enough sources of information for the committee members; where necessary, these could be complemented by direct communication with an institution's internal control functions.

- The requirement under point (b) referring to "*any breaches*" would include too many occurrences if it were to cover any breach of any limit. It should refer to "*material breaches*".

- With regard to point (d), it should be noted that the risk committee is a committee established by the supervisory body. The basis here too should therefore be the responsibilities within the dual board structure. Involvement of internal control functions in the relevant processes is primarily the responsibility of the MBMF and not the MBSF, which merely examines whether the internal control functions have been properly involved. Instead of the term "*ensure*", the right term here would be "*oversee*".

**Paragraph 47**

- The requirements under points (a) and (d) should be reconsidered for a two-tier structure, where the supervisory board does not set the risk appetite, strategy or corporate culture. For example, there is a requirement under point (d) for the risk committee to advise the supervisory board on risk strategy although this is set by the management board.

- According to point (g), the risk committee has to "*examine the alignment between all financial products and services offered to clients and the business model as well as the risk strategy of the institution*". In addition, it is required to "*assess the risks associated with the offered financial products and services and examine the alignment with the prices assigned and profits gained from those products and services*". This, again, is an operational task of the management board. The risk committee's job should hence be overseeing but not executing. The word "*examine*" should therefore be replaced by "*oversee*". Under German banking supervisory law, the risk committee is, for example, required to "*monitor whether conditions in customer business are in line with the undertaking's business model and risk structure*" (Section 25d (8), sentence 3 of the German Banking Act). Such monitoring cannot cover every single product, as this would impose an unreasonable burden on the risk committee. It should be made clear that collective examination and assessment are allowed.

**Comments on the EBA Draft Guidelines on internal governance**

- With regard to point (g), "*all*" should be removed from "*financial products*" to factor in reasonable materiality and product grouping.

**Paragraph 49**
This describes the information for a risk committee, which would be excessive for a nomination committee that has a hugely different purpose. The respective requirements should be separated for the purpose of clarity.

**Paragraph 50**
Point (a) should not refer to "*the institution's internal quality control*" but to "*the institution's internal control framework*" or "*internal control mechanisms*", as provided for in CRD IV (cf. Article 74 thereof). A requirement for the audit committee to monitor the effectiveness of internal quality control would be much too operational in nature and unduly burdensome.

Furthermore, the internal audit committee is only mandated to look at the effectiveness of the internal audit function in terms of reporting. It should be clarified which function should assess the broader effectiveness of internal audit.

**Paragraph 51**
This paragraph states that competent authorities may allow institutions that are not considered significant to combine the risk committee with the audit committee. As there is no general requirement for non-significant institutions to establish the committees mentioned, no permission from competent authorities should be needed to combine any voluntarily established committees. Clarification on this point would be welcomed.

**Paragraph 53 ff.**
Under the German dual board system ensuring an appropriate organisational and operational structure is primarily the responsibility of the management (and not of the entire management body including its supervisory function). Contrary to what paragraph 19 says, the guidelines are thus not worded neutrally system-wise. We request the addition of an opening clause.

**Paragraph 54**
With regard to the requirement for all members to know how responsibilities are divided up between all key function holders, we would strongly argue that a materiality threshold should be introduced for significant firms with large numbers of individuals.

**Paragraph 55**
According to the first sentence, the management body should "*assess how the various elements of the organisational and operational structure complement and interact with each other*". Implementing this requirement would impose a heavy burden in practice that would not be balanced out by any real benefit. The requirement that "*the structure should not impede the ability of the management body to oversee and manage effectively the risks the institution or the group faces and of the competent authority to effectively supervise the institution*" should suffice.

**Paragraph 57**
The wording "*should fully know and understand the organisational and operational structure of an institution*" is, in our view, much too far-reaching. It would mean that the members of the management body would have to know all organisational units, right down to the smallest teams or staff level,

including functions/responsibilities and processes. This is not necessary, nor – particularly where large and complex institutions are concerned – is it feasible. We recommend changing the wording to "*should know and understand the main features of the organisational and operational structure of an institution"*.

Furthermore, we suggest deleting the wording "*and ensure that it is in line with its approved business and risk strategy, and risk appetite*", as understanding the structure of the institution in line with risk appetite is a confusing concept without any further explanation.

**Paragraph 60**
The requirement for all board members to "*know the purpose and activities of its different entities*" is unachievable in certain circumstances. As the largest consolidated groups in the EU may have over 20,000 legal entities (including SPVs) within their group, we recommend limiting this requirement so that board members would be required to know the purpose and activities of only the most material entities within their group.

**Paragraph 62**
We suggest deleting sub-points (a)-(c), given that the level of detail exceeds that for other risks such as market or credit risk.

**Paragraph 63 ff.**
The draft guidelines are often very vague and unspecific and appear impractical in some cases. That goes for what they say both with regard to institutions and management, e.g. paragraph 63 d): institutions should take into account "*the extent to which the customer's request to set up a structure gives rise to concern*".

As the measures are rather unspecific as a whole, differing national implementation in the EU creates an uneven level of protection against non-transparent companies.

As regards the reporting to competent authorities under paragraph 67 b) of the draft guidelines, it should be noted that associated data protection and/or tax secrecy issues that may impede such reporting are not addressed.

It should also be noted that it is very often virtually impossible for financial institutions to actually identify such non-transparent companies in practice because of the efforts these companies make to conceal their activities by exploiting the law in certain jurisdictions. For this reason, no excessive or virtually unfulfillable duties should be imposed on financial institutions in general, especially as it must be remembered that financial institutions are not (tax or law-enforcement) authorities, do not perform any predominantly sovereign functions and consequently have no official 'investigative powers' either. Both the OECD and the EU have acknowledged this and stipulated in the Common Reporting Standard (CRS) and the EU Mutual Assistance Directive (both are regulation governing the automatic international exchange of information in tax matters) that, where accounts are held by legal entities, the legal entity has to issue a so-called "self-certification" stating whether it is an active or passive entity and, if it is a passive entity, to additionally indicate the persons controlling it.

The same goes for other vague passages in the guidelines which mean in some cases that institutions will be burdened with what are, theoretically, virtually unlimited obligations, e.g. paragraph 63 a): "… *institutions should take into account … the extent to which the jurisdiction in which the structure will be set up complies effectively with international standards on tax transparency, anti-money laundering and*

*countering the financing of terrorism*". This requirement is, in our view, excessive and its implementation is unfeasible in practice.

**Q4: Are the guidelines in Title II regarding the internal governance policy, risk culture and business conduct appropriate and sufficiently clear? [paragraphs 70-109]**

**Paragraph 70/Annex 1**
The requirements to be met by an institution's internal governance policy and the requirements to be met by the supervisory body when it comes to overseeing the internal governance policy are expanded significantly. We believe that the requirements as a whole go too far and ask for removing the whole Annex.

Furthermore, particularly the aspects set out in Annex I, 6 (c) and (d) ("*weaknesses identified by each internal control function/measures taken to address them/recommendations made by the internal audit function"*) are not, in our view, part of the internal governance policy but, instead, the result of internal review and assessment processes that are included in the accompanying reporting. We therefore recommend slimming down the requirements accordingly.

Furthermore, it would be disproportionate and also make little sense to require a large and complex institution to produce such an internal governance policy, since the content needed in each section would be highly complex to document and impose an unnecessary administrative burden on such institutions. Large and complex institutions already clearly document internal governance arrangements by way of several targeted policies, maintained by many functions. We would therefore request the EBA to consider allowing institutions to defer to existing policies (e.g. financial reports), to which multiple internal committees also provide input. Alternatively, it would be more proportionate to request firms to instead produce a simple mapping document which links to existing policies/materials. On the other hand, it should also be possible for the governance policy to comprise several documents (constitution, business rules of procedure, internal organisational/work instructions).

In addition, the requirement (with regard to the internal governance policy) in paragraph 70 for the supervisory body to be "… *responsible for overseeing its implementation and that it is fully operating as intended …*" goes too far in a two-tier system. The supervisory body does its job outside an institution's operational activities. Whether requirements are really fully implemented and effective is something that the members of the supervisory body are ultimately unable to determine. The requirements should be clarified with this in mind.

With regard to the content of the internal governance policy set out in Annex 1 of these draft guidelines, the weaknesses and recommendations of control functions are likely to be confidential and rapidly changing. It would therefore be inappropriate to include this information in such a transparent document. It should be clarified what is meant by "*free provision of services*" in [Annex 7(e)].

**Paragraphs 75-79**
It should be clarified whether the expectation is for firms to draft separate policies for every non-EU entity within prudential consolidation and have a central group policy applying to all EU entities. We would argue that a group-wide policy would suffice.

We also recommend that in the case of groups of institutions with holding company structures the consolidating institution should ensure that consistent (paragraph 75) and robust (paragraph 76)

governance "*arrangements, processes and mechanisms*" are established in all subordinate (fully or partly consolidated) companies. In our view, a clear reference to the criteria set out in Title III "*Proportionality*" should be included here. When looking at the institutions within a group individually, these criteria should be taken into account in assessing consistency and robustness. In addition, it should be made clear that consistency is not the same as completeness. Within a group, institutions should be allowed to seek a different breadth and depth of arrangements, processes and mechanisms in line with given proportionality to the group and their individual specificities, as long as these are not inconsistent with the holding company's governance policy.

**Paragraph 75**
It should be clarified whether a 'comply or explain' approach would meet the "*consistent and well integrated*" requirement (i.e. as set out in FAQs of EBA Internal Governance 2011 version).

**Paragraph 77**
According to the first sentence, the consolidating institution is required to ensure that all group entities comply with all specific requirements in any relevant jurisdiction. This is practically impossible. The consolidating institution cannot possibly know all specific requirements in a jurisdiction. It is up to the management body of the group entity to ensure compliance with local laws and regulations. It should also be noted that there are also entities within a group, e.g. joint ventures, where there is no controlling influence. The consolidating institution can therefore only exert its influence by urging the group entities to comply with local laws and regulations. We recommend amending the wording of the requirements accordingly.

**Paragraph 85**
In our opinion, the requirement to establish a code of conduct does not make sense for all institutions (see in this context our comments on paragraph 19). We take a critical view in general of the fact that the term "*risk culture*" is tied to ethical and moral considerations. Moral aspects are difficult to capture and continuously subject to social fluctuations; there are sometimes highly divergent views on the standards set under such a code of conduct.

A code of conduct is not appropriate for small institutions. Such a catalogue of acceptable and unacceptable behaviours is neither realizable nor necessary. We do not think that EBA aims institutions to copy existing codes. Therefore it would generate an unacceptable burden to establish such a code of conduct.

It should also be noted that the code of conduct is also to apply to external services providers. We wish to point out that it is not clear how agreement on a code of conduct can be achieved, overseen and, if necessary, enforced. At the same time, we would welcome clarification on who is to be responsible for monitoring compliance with the code of conduct and who is to offer staff training courses on compliance, along with an explanation of the consequences of non-compliance.

**Paragraph 87**
The requirement under point c to define acceptable and unacceptable types of behaviour is, in our view, neither workable in practice nor necessary. Listing all acceptable and unacceptable types of behaviour would impose an unreasonable burden and ultimately assume an unmanageable dimension. What is more, not all situations or cases that might theoretically occur can be defined in advance – the list would inevitably be incomplete. The internal governance guidelines already contain various requirements and

instruments intended to ensure both compliance with legal and internal standards and ethically correct behaviour. This point should therefore be deleted.

**Paragraphs 90-103**
The requirement to disclose every case of a conflict of interests (and how they are mitigated) would be excessively burdensome. Materiality thresholds in which competent authorities envisage the requirement in question should be clarified.

**Paragraph 91**
In accordance with Article 91 (4) of CRD IV, we request an exemption not only for management or supervisory mandates in institutions that belong to the same institutional protection scheme (point (b)) but also for management and supervisory mandates within the same group (cf. point (a)). The conflicts of interest mentioned do not exist in these cases.

**Paragraph 94**
The organisational measures required under points (b) and (c) would impose a considerable bureaucratic burden on small institutions in particular. The requirement to take such measures should therefore be confined to significant institutions.

**Paragraphs 104-105**
Competent authorities are to establish mechanisms for reporting breaches of regulatory requirements. Staff can already contact competent authorities direct today, so that 'encouraging' them to do so will open the door for particular discontented employees to simply vent their frustration to competent authorities. The existing rules on whistleblowing are adequate.

**Paragraph 107**
This paragraph emphasises concentration risk in assessment of outsourcing requirements. Outsourcing to multi-client services providers usually entails concentration risk, however. Drawing attention especially to such risk is therefore not a suitable defining criterion, in our view, as it is likely to make differentiating between significant and insignificant outsourcing difficult in many cases.

**Q5: Are the guidelines in Title III regarding the principle of proportionality appropriate and sufficiently clear? [paragraphs 110 – 111]**

**Paragraphs 110 and 111**
These passages should precede the text of the guidelines; and it should be made clear that the proportionality principle applies to all requirements set in the guidelines.

**Paragraph 112**
In our view, "*group structure*" should be included as an additional aspect. The requirements for an institution at solo level should be seen within the context of the group's internal governance. Particularly where there is a centralised governance approach, this prevents individual institutions' internal governance arrangements from being perceived separately as inappropriate.

Along the same lines as above, we would welcome it if the list under point (h) were extended to include groups of institutions and group-wide risk strategies, risk appetites and risk profiles. Groups of institutions should be free to gear individual institutions' risk strategies to the group's overall strategic approach.

**Comments on the EBA Draft Guidelines on internal governance**

**Q6: Are the guidelines in Title IV regarding the internal control framework appropriate and sufficiently clear? [paragraphs 113-198]**

**Paragraph 113**
In line with our remarks on paragraphs 75/76 and 112, we should welcome clarification here that the proportionality criteria may be applied to groups of institutions in such a way that the requirements for an internal control framework are developed at group level and individual institutions adhere to these.

**Paragraph 116**
Irrespective of the management body's responsibility for developing and overseeing an adequate and effective internal control system, it must be ensured that the management body is properly involved in the operational processes, taking into account the principle of proportionality. The "*proper involvement*" of the management body is currently standard practice in Germany. The requirement to obtain express management body approval for individual work directives in the context of the internal control system could impose a needless additional bureaucratic burden at individual institution level. At numerous points in various other EBA guidelines or standards, as well as in the CRR, the involvement of the management body is likewise explicitly called for. This may lead, overall, to a broad need for coordination also on operational issues that are not the primary responsibility of the management. We therefore call for wording that allows institutions more flexibility when it comes to the involvement of the management body. It could, for example, be made clear that general rules are meant here and not instructions in day-to-day business.

**Paragraph 122**
Internal audit, as an independent control function, performs a key task for the management body. In a dual board structure we believe it is appropriate for internal audit – while preserving the required independence and the right of access by the supervisory body – to be accountable to the management body.

**Paragraphs 123/150/193**
There is in general no requirement under the distribution of responsibilities within a German stock corporation for the head of the IAF/RMF to report directly to the supervisory body; this needs to be regulated by law or a company's constitution.

**Paragraph 124**
The supervisory body is to approve the appointment or removal of the heads of internal control functions. This is in line with current rules – as far as the risk management function (RMF) is concerned, at any rate. However, in the German dual board structure how executive positions are filled is the primary responsibility of the management body. Contrary to what paragraph 19 says, the guidelines are thus not neutral system-wise. We would welcome the addition of an opening clause. In addition, the current provision of Article 76 (5) of CRD IV already stipulates that "*The head of the risk management function shall not be removed without prior approval of the management body in its supervisory function*." To avoid redundancies, we believe that this passage should not be included again in the guidelines.

**Paragraph 130**
A "*holistic institution wide risk management framework*" is called for as part of the "*overall internal control framework*". We request clarification on separation of the risk management framework and the internal control framework.

**Comments on the EBA Draft Guidelines on internal governance**

**Paragraph 131**
This paragraph should permit institutions to consider the appropriate levels of risk, subject to other regulatory requirements. Certain risks are managed on an entity basis and they offset each other or are mitigated through diversification, so that a business line approach may not be most appropriate.

**Paragraph 141**
While the high-level framework should be documented in the risk management framework and approved by the management body, it would impose an administrative burden were every individual detail and changes thereto to require such approval in a significant institution. We expect that such a level of detail is not intended and would appreciate clarification to this effect.

**Paragraph 143 ff.**
This paragraph sets requirements for the new product approval policy (NPAP) and for material changes to processes and systems. According to the first sentence, the NPAP should address "*the development of new markets, products and services and significant changes to existing ones*". The second sentence says that an institution should also have "*appropriate change policies for material changes to processes and systems*". The following paragraphs 144ff. do not, however always differentiate consistently between both requirements, so that it is unclear whether the requirements set in the individual paragraphs relate solely to the NPAP or to the NPAP and changes to processes and systems. Only paragraphs 146 and 147 expressly refer to the NPAP. Paragraphs 144 and 145, in contrast, merely refer in general terms to policies. Paragraph 148, on the other hand, refers to "*significant changes to existing products, processes and systems*", although it is unclear whether, in addition to the NPAP ("*significant changes to existing products*"), "*material changes to processes and systems*" within the meaning of paragraph 143, second sentence are meant. We therefore recommend clearly separating the requirements for the NPAP and changes to processes and systems in the guidelines. The compliance and risk management functions have to be involved where both the NPAP and changes to processes and systems are concerned. This is in line with the requirements already applying today. In addition to both internal control functions, all organisational units subsequently involved in workflows, as well as the IAF, are already usually included in the NPAP in practice today. What is new is that for the NPAP (and, as the case may be, for material changes to processes and systems – see sentences 1 and 3) an institution should, under paragraph 145, have "*specific procedures for assessing compliance with these policies*" and that "*this should include a systematic prior assessment and approval by the compliance function, including a written opinion from the head of compliance*". In addition, paragraph 181 in section 15 of the EBA guidelines requires that "*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 requirements for the compliance function within the NPAP are appropriately and adequately defined in paragraph 181 of section 15. No "*specific procedures for assessing compliance*" are therefore necessary. We also believe that a "*written opinion from the head of compliance*" in the sense of final approval of the NPAP by the compliance function is inappropriate. This applies particularly if paragraph 145 goes beyond the NPAP to cover "*material changes to processes and systems*". The compliance function does not have overall responsibility for the NPAP. The compliance function's contribution to the NPAP is instead only one element – albeit an important one – of the NPAP. We therefore recommend deletion of this passage.

**Paragraphs 144/145**
If interpreted narrowly, the proposed requirements for the compliance function would mean that the head of the compliance function or a person authorised by him or her, together with the risk management

function, would effectively have to approve new products or material changes to existing products. In our view, this goes well beyond the tasks of the compliance function and the risk management function, particularly as all the relevant organisational units of an institution are involved in the new product process (NPP). We request clarification to the effect that the compliance function and the risk management function only have to be involved in the NPP within the limits of their respective remits.

**Paragraph 148**
We recommend dropping the required scenario analysis, i.e. the wording "*under a variety of scenarios*" should be deleted. Given the large number of scenario analyses already required, the additional analyses called for here – now even for fictive positions – would impose an unreasonable extra burden while delivering only limited added value.

**Paragraph 154**
This paragraph calls for a group-wide "*holistic view on all risks*" ensuring compliance with the risk strategy. In our view, the materiality principle should be reflected in the way the risk strategy is designed. The requirement in the final sentence should hence be confined to material risks.

**Paragraphs 154, 161 and 164**
In these paragraphs the term "*all risks*" is used. We believe that, with the materiality principle in mind, the requirement should be confined only to "*material risks*" and therefore request that the wording be amended accordingly. Furthermore, it should be noted with regard to paragraph 161 that not all risks – as called for – can be measured (particularly non-financial risks). Clarification to this effect would be welcomed.

**Paragraph 156**
The risk management function cannot ensure that the risk appetite is appropriately translated into specific risk limits, since the management body decides on the limits proposed by the risk management function. The risk management function can thus only ensure that appropriate proposals for translating the risk appetite into appropriate specific limits are submitted to the management body. We therefore request that this paragraph be amended accordingly.

**Paragraph 161**
We request deletion of the word "*mitigated*" in connection with the "*RMF should ensure*". In many cases, the risk management function cannot ensure that risks are mitigated, as the decisions in this respect are taken either by other departments or the management body. The risk management function's usual tasks, on the other hand, include making risks transparent, informing the management body and the departments affected thereof, and proposing risk-mitigating measures. This understanding of its functions is also acknowledged, in our view, in paragraph 166.

**Paragraph 170**
This requirement widens the risk management function's remit. Such action is currently the responsibility of the compliance function. We therefore request clarification that this requirement does not necessarily have to be implemented by the RMF.

**Paragraph 172**
We welcome the express inclusion at this point of the proportionality principle with regard to appointment of the head of the RMF. This gives small institutions the required leeway when it comes to framing responsibility for risk management and compliance. May we, however, draw attention in this respect to

the unclear priority ranking of proportionality for the internal control framework that we refer to in our remarks on paragraph 175.

**Paragraph 174**
It should be clarified that this paragraph relates to decisions made by the management body (as per paragraph 173) and not to any decisions in which the CRO is involved.

**Paragraph 175**
The embedment of the proportionality principle in the requirements for the compliance function is unclear. Proportionality criteria as listed in Title III are to generally apply to the establishment of the entire internal control framework, to which the compliance function also belongs (paragraph 113). However, we fail to understand why, when siting the compliance function (paragraph 176) – and only then with regard to this function – express reference is again made to proportionality criteria listed in Title III. This could mean that proportionality criteria only have to be taken into account within the scope of paragraph 176 and not where other compliance function standards are concerned. Otherwise, because of the general reference in paragraph 113, this specific reference at this point could have been dispensed with. We should therefore welcome it if the EBA could clarify how the general application of the proportionality principle and specific references to proportionality rank in priority.

**Paragraph 176**
We are strongly opposed to the evidently envisaged restriction on the possibility to combine the compliance function with other units. Unlike in the current EBA guidelines, there is no longer any mention of the fact that, where smaller and less complex institutions are involved, the compliance function can be combined with the risk management function or other supporting functions (e.g. human resources or legal division) or assisted by these. Instead, this paragraph merely says that, taking into account the proportionality criteria listed in Title III, the compliance function may be combined with the RMF or the legal division or assisted by the RMF. Such a restriction on siting the compliance function – if actually intended – would fly in the face of reality at smaller institutions, however.

Particularly at smaller institutions which have only a small number of staff, such a requirement is simply impracticable. The current German practice whereby only the IAF, being outside the internal control system, is excluded from the compliance function along with market trading units is appropriate in our view. So far, no problems at smaller institutions that need to be addressed by restricting the right to combine the compliance function have come to light in practice.

**Paragraph 178**
The requirement for institutions to have a well-documented compliance policy that should be communicated to all staff stems – like the implementation of a compliance monitoring programme called for in paragraph 180 – from the approach adopted by large (internationally operating) banks and should not be applied in an unreflected manner to small institutions. In their case, it should suffice if special standards or policies are adopted for special areas of compliance, e.g. securities trading, money laundering or data protection, and are regularly communicated to staff. A specific compliance policy focusing on general legal risks (paragraph 179) that is to be communicated to all staff would, on the other hand, be an example of disproportionate regulation, particularly for smaller institutions. It should be sufficient in this respect if the compliance function addresses the relevant risks by way of regular analysis and reporting and involves the units concerned where necessary. Express reference to the proportionality criteria in Title III would be welcomed here.

## Comments on the EBA Draft Guidelines on internal governance

**Paragraph 180**
To avoid any unreasonable burden, we believe that the requirement to have a structured and well-defined compliance monitoring programme should be modified so that, in line with the proportionality principle, such a compliance monitoring programme takes into account the size and complexity of an institution.

From the perspective of small institutions with a small number of staff operating only locally, the requirement to implement a compliance monitoring programme as specified in paragraph 180, i.e. the kind usually operated by large banks, would be excessive. Express reference to the fact that such a programme is only necessary for institutions where called for from a proportionality perspective would therefore be welcomed. In this context, it should be borne in mind that process-independent inspections are the task of the internal audit function and that its work does not need to be duplicated by the compliance function. On the other hand, we expressly welcome the reference to cooperation and an exchange of information between the compliance function and the risk management function since this will, in our view, allow more efficient and better-quality monitoring.

**Paragraph 182**
Institutions can merely bring their influence to bear on subsidiaries so that they comply with local laws and regulations. Actual compliance with local laws and regulations is the responsibility of each subsidiary itself. The word "*ensure*" should therefore be replaced by "*provide that*".

**Paragraph 185**
Widening the scope of the internal audit function to cover all entities would lead to a number of non-material entities having to be taken into account. We recommend wording paragraph 185 more narrowly as follows: "*The IAF should independently review the compliance of all activities and units of an institution including outsourced activities with institutions' policies and procedures and that should ensure that each material entity within the group fall**s** within the scope of the IAF.*"

**Paragraph 189**
The term "*unfettered access*" may imply a greater obligation than intended, so including the term "*upon request*" would reduce the practical implementation issues for banks.

**Paragraph 194**
In line with our remarks on paragraph 113, we should welcome clarification here too on the application of the proportionality principle to groups of institutions. Business continuity management should be sound at group level and both appropriate and effective at individual level.

**Paragraph 198**
Institutions are to be required to adequately document their contingency, business continuity and recovery plans and to make them available to the business lines and the RMF. These plans should be "*stored on systems that are physically separated and readily accessible in case of contingency*". This wording should be amended to clarify the type and scope of physical separation required. It is unclear whether it means a general separation of 'contingency documents' from the documents normally made available within institutions (e.g. the regular handbooks) or whether it is merely referring to the requirement to hold separately accessible back-up.

## Comments on the EBA Draft Guidelines on internal governance

**Paragraph 199 ff.**
The requirement to communicate strategies, policies and procedures to all the staff of an institution should be modified to include a reference to the fact that this requirement is satisfied by electronic communication (e.g. on an institution’s in-house intranet).