



Abs.: Aareal Bank AG, Paulinenstr. 15, 65189 Wiesbaden
European Banking Authority
One Canada Square (Floor 46)
Canary Wharf
London E14 5AA| UK

January, 18th 2017

**Comments of Aareal Bank on EBAs Consultation Paper:
Draft Guidelines on internal governance**

Dear Sir or Madam,

We appreciate the opportunity to submit our opinion on your draft guidelines on internal governance and would especially like to raise the following points:

- We would like to ask EBA to bear in mind the well separated duties between the management and the supervisory function, determined especially in the German company law.
 - Proposals like a responsibility of the supervisory function in order to ensure the effectiveness of the institution's governance framework put the responsibility of the management function in question.
 - Direct reporting lines from the internal control functions to the supervisory function are breaching the well allocated responsibilities to which these functions are accountable. The management function has to develop and implement the risk management framework and therefore, even to organise the internal control functions as well as to select their heads. In consequence, they should be the addressees of any reporting,

(2)

and the internal control functions should remain accountable to the management function. Complementary, the supervisory function should not have any prior approval obligation on their positions since the management function is in charge of the head's selection.

- Well-allocated responsibilities should also lead to a clear distinction between duties of different committees which is why either the risk, nomination or audit committee should have separated tasks. To concern the audit and the risk committee with the audit plan as well as the intermixture of duties in risk issues between the risk and the nomination committee is not in line with this idea.
- Furthermore, we would like to ask EBA to adjust some of the provisions as to the intention of the three lines of defence-model. If the compliance function has to analyse all policies and the internal framework, it substitutes the internal audit function. If the risk management function's responsibility should be increased to the identification and managing of any risks, it is obliged with a duty of the business lines as first line of defence which puts its independence in question.
- We also raise the increase of duties of the internal control functions in general to your attention. In our opinion, to ensure the identification of all risks, to ensure compliance with all laws, to review all activities is objective of a framework (e.g. internal control framework, risk management framework) but not of a function with limited staff.

We appreciate your considering of our following elaborated position in advance and are open for any further discussion on these points.

Table of Content

Q1: Are the guidelines regarding the subject matter, scope, definitions and implementation appropriate and sufficiently clear?.....	6
Definition of Key function holders.....	6
Definition of heads of internal control functions.....	6
Q2: Are there any conflicts between the responsibilities assigned by national company law to a specific function of the management body and responsibilities assigned by the Guidelines, in particular within paragraph 23, to either the management or supervisory function	7
Ensuring the effectiveness of the institution's internal governance framework	7
Direct reporting from RMF, CF and IAF	7
Direct accountability of IAF	8
No remove of internal control function's heads without prior approval of supervisory function.....	9
Q3: Are the guidelines in Title I regarding the role of the management body appropriate and sufficiently clear?	9
I. Duties of the (entire) management body.....	9
Implementing measures to devote sufficient time on risk issues	9
Transparency of structure	10
II. Duties of the management body in its supervisory function	10
Ensuring the effectiveness of the institution's internal governance framework (equal to answer to Q2)	10
In regard of para 24 g please refer to our answer to Question 2: Direct reporting from RMF, CF and IAF into account.....	11
Assessment of internal governance policy	11
III. Rules for the committees of the management body in its supervisory function	11
Diverse composition of different committees.....	11
Independence of members	12
Rotation of memberships	12
Expertise of members	13
Doubling of duties of committees	13

IV. Rules for the risk committee.....	14
Information on any breaches in risk issues	14
Ensuring the proper involvement of internal and external advice	14
Examining the alignment between all financial products and services.....	15
V. Rules in regard of complex structures, non-standard or non-transparent activities	15
Para 63 ff., 68 avoiding setting up complex and potentially non-transparent structures.....	15
Q4: Are the guidelines in Title II regarding the internal governance policy, risk culture and business conduct appropriate and sufficiently clear?	16
I. Internal governance policy.....	16
The introduction of an internal governance policy for an overview about the corresponding framework.....	16
For further comments on para 72 and the conflict with the three-lines-of-defence model, please see our answer to Q6.....	17
II. Rules for corporate values and code of conduct.....	17
Definition of acceptable and unacceptable behaviours.....	17
Q5: Are the guidelines in Title III regarding the principle of proportionality appropriate and sufficiently clear? When providing your answer please specify which aspects and the reasons why. In this respect, institutions are asked to provide quantitative and qualitative information about the size, internal organization and the nature, scale and complexity of the activities of their institution to support their answers.....	18
Q6: Are the guidelines in Title IV regarding the internal control framework appropriate and sufficiently clear?.....	18
I. Rules for all internal control functions	18
Inconsistencies with the three lines of defence-model.....	18
For our comments on the direct reporting rights to the management board in its supervisory function and direct accountability of IAF, please see our answers to Q2.	19
II. Rules for the RMF	20
The extension to future risks	20
Control of external behaviour	20
III. Rules for the CF	20

CF's role in the new product approval policy (NPAP)	20
III. Rules for the IAF	21
Reporting to the risk committee	21
The group wide review of all activities and units.....	21
IV. Rules for the business continuity management	21
Q7: Are the guidelines in Title V regarding transparency of the organization of the institution appropriate and sufficiently clear?.....	22
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?.....	22

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

Definition of Key function holders

We support the definition of key function holders as persons who “have significant influence over the direction of the institutions, but who are not members of the management body nor the CEO. This should include the heads of the internal control functions and the CFO, where they are not members of the management body, and, where identified on risk-based approach by institutions, other key function holders.”

We would like to ask ESMA and EBA to set out in this definition that having significant influence on the direction of the institution typically does not include heads of internal functions like human resources, legal etc. Additionally, the heads of business lines are also generally not in scope, since in two-tier-systems decisions about the direction of the institution are taken within the management board (management body in its management function) according to company acts like art. 76, 77, 91 of the German Public Limited Companies Act. Heads of internal functions are usually only in charge to decide within derived competences, maybe about credits until a specific amount, but not about the (strategic) direction of the institution. They might prepare such decisions though, but may not eventually decide upon.

This might differ to one-tier systems where many managerial responsibilities can be derived to special officers (like a CCO not member of the management body). In this case, decisions could have significant influence on the direction.

Definition of heads of internal control functions

By defining the heads of the internal control functions as well as in the whole following paper, EBA concerns the risk “management” function. We ask EBA to clarify its intention by replacing the term risk “control” function, used in the current EBA Guidelines 44 from 2011, by risk management function without changing the subject. Does risk management function still encompass the same department as the risk control function?

We are uncertain whether different implications result from these terms. By comparing the corresponding BCBS papers we recognise even not a clear application of the terms. In BCBS

Standards for Minimum capital requirements for market risks (p. 20 footnote 15) from January 2016 risk control function is mentioned while BCBS Guidelines Corporate Governance principles for banks from July 2015 as well as in BCBS "Guidance on the application of the Core Principles for Effective Banking Supervision to the regulation and supervision of institutions relevant to financial inclusion" from September 2016 concerns the risk management function.

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

Ensuring the effectiveness of the institution's internal governance framework

In the German corporate governance-system the management board is responsible for ensuring the effectiveness of the institution's internal governance framework while the supervisory board is (only) obliged to assess and monitor the implementation of the institution's internal governance framework. The supervisory board receives information by the management function or the auditors and relies on its own investigations and assessments of the information provided to identify any deficiencies of the internal governance framework, only to the extent possible though. Hence, the supervisory function is not capable to ensure the effectiveness since its controls are restricted to such information.

We would therefore like to ask EBA to transfer the obligation to ensure the effectiveness from para 24h to the tasks of the management body in its management function and reduce para 24h to the extent of a periodical review by the supervisory board.

Direct reporting from RMF, CF and IAF

In the German corporate governance-systems it is the responsibility of the management board to inform the supervisory board. The management board must provide for an internal reporting system in accordance with art. 90 of the German Public Limited Companies Act to be properly informed and based on this having an effective risk management framework implemented. The management board then derives a respective reporting for the supervisory board.

Against this, the supervisory board's duty is limited to oversee and monitor the members of the management body, with respect to their responsibility on developing and implementing a risk management framework. This includes the supervisory board's task to assess whether this risk management framework is effective and to check if responsibilities for the controls have been appointed.

Direct reporting lines and accountability from staff below management board level to the supervisory board is not complying with this principle and are not providing any advantage. The benefit of (at least) the German corporate governance-system is that the supervisory board has a direct counterpart responsible for all questions or enquiries the members of the supervisory board may have. Please bear in mind that there is a clear separated division of responsibilities. That also avoids to have the unfavourable situation of a conflict of interest for the heads of internal control functions to decide to whom report first. Giving these heads direct access to the supervisory board may from an organisational point of view lead to mistrust the management board's members without cause.

We would therefore like to ask EBA to abstain from the ability to report directly to the supervisory board (para 150, 168, 175, 193) and to acknowledge the current supervisory function's rights to ask the heads of internal control functions directly as sufficient. This right is appropriate in case of a need to receive information without taking a circuit.

Direct accountability of IAF

According to para 122 the heads of Risk Management Function (RMF) and Compliance Function (CF) should be directly accountable to the management board and the head of the Internal Audit Function (IAF) should be directly accountable to the supervisory board. However, the appointment of the head of the IAF is intended to remain part of the management board's duties. Thus, the management board would remain in charge for the remuneration of the head of the IAF and the composition of the IAF staff. These competences are inextricably linked to the accountability.

We would like to ask EBA to elaborate why this procedure is deemed beneficial for the corporate governance-system and provided that this may be deemed as advantageous how this could justify the breach of base principles of such corporate governance-systems. As we currently may not follow the idea and the rationale of the aforementioned draft requirement we would like to ask for deleting para 122.

No remove of internal control function's heads without prior approval of supervisory function

Supplementing our above well-elaborated position and in especially facing that the management body in its management function should stay in charge to appoint a new head of an internal control function without the prior approval of the supervisory function, we would like to ask EBA to delete the provision in para 124. The organisation of the internal control functions and the selection of their heads is part of the risk management framework. To implement this framework is duty of the management function but not of the supervisory function. Mere information from the management function to the supervisory function should be sufficient.

Furthermore, the independence of the supervisory board is far greater if the supervisory board is not involved in the appointments and reporting lines of function holders below management board level. If the supervisory board is obliged to appoint or to vote on the appointment of heads of internal control functions, the supervisory board's independence is threatened when assessing this person. This may be the case, since a member of the supervisory board has proposed him for its appointment.

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

I. Duties of the (entire) management body

Implementing measures to devote sufficient time on risk issues

According to para. 19 b the management body should also implement measures to ensure that the management body devotes sufficient time to risk issues. We ask EBA to make clear, what "measures" mean and why "time" is in question?

It is a crucial obligation of members of the management body to take decisions on a sound and well-informed basis (para 28, 30), which means to consider, whether they know and have understood all necessary aspects to take their decision. If they haven't, they could be liable for damages resulting from this decision. We don't know what measures in addition to this obligation should be. We assume this is why art. 76(1) CRD IV also only requires that the management body devotes sufficient time without implementing specific measures.

Furthermore, if they need time to gather sufficient information so they have to take it before they decide.. If they are already informed and are able to consider all necessary aspects by taking a decision on a risk issue, they must be allowed to use only short time. In addition, it depends on the materiality of the risk issue how much information and how much consideration is needed to decide on it. Low risk issues require less time and information than medium or high risks.

Hence, we would like to ask EBA to delete this “new obligation”.

Transparency of structure

According to para 58 the management body should ensure that the structure of an institution and, where applicable, the structures within a group, are clear, efficient and (new:) transparent to institution’s staff, shareholders, other stakeholders and to the competent authority.

We ask for clarification which detail level this provision is intended to require. Should the structure be transparent to all stakeholders in the same degree as to the members of the management body according to para 53? Pursuant to this provision a suitable and transparent structure should promote and demonstrate the effective and prudent management of an institution at individual, sub-consolidated and consolidated level. Do also the reporting lines and all competences including the internal control framework have to be demonstrated / being transparent, although art. 106 para 2 only requires to disclose the general structure? Additionally, we do not know the scope of “other stakeholders”. Who should be informed in this detail?

Neither shareholders nor stakeholders such as the public or customers have a need for a higher level of transparency than already required by art. 106 para 2 CRD IV, directive 2013/34/EU and (inter)national accounting standards.

II. Duties of the management body in its supervisory function

Ensuring the effectiveness of the institution’s internal governance framework (equal to answer to Q2)

In the German corporate governance-system the management board is responsible to ensure the effectiveness of the institution’s internal governance framework while the supervisory board only has to assess it and monitor the implementation by the management board. Another approach is impossible, because the supervisory board can’t ensure the effectiveness. It receives information by

the internal control functions or the auditors and makes its own investigations to identify any deficiencies of the internal governance framework but only to the extent possible.

We, therefore, ask ECB to transfer the obligation to ensure the effectiveness from para 24h to the tasks of the management body in its management function and reduce para 24h to the periodical assessment by the supervisory board.

In regard of para 24 g please refer to our answer to Question 2: Direct reporting from RMF, CF and IAF into account.

Assessment of internal governance policy

According to para 24 h the management body in its supervisory function should ensure and periodically assess the effectiveness of the institution's internal governance framework and take appropriate steps to address any identified deficiencies. The draft EBA guidelines have introduced the term "policy", e.g. in para 73, instead of "framework". Perhaps, the term in para 24 h has to be adjusted.

III. Rules for the committees of the management body in its supervisory function

Diverse composition of different committees

The EBA guidelines are intended to require that committees are not being composed mostly of the same group of members which form another committee (s. para 37). We would like EBA to delete this provision. You have to take into account, the interaction between the obligation to set up at minimum four committees (risk, nomination, audit and remuneration) and the obligation to have at least one member of another committee within and only a less amount of members in a management body in its supervisory function. In addition, in any case in Germany but perhaps even in other countries every committee has at least to consist of three members (Koch in Hüffer/Koch, § 107 AktG, Rn. 29; Spindler in Spindler/Stilz, § 107 AktG, Rn. 98) and has only a quorum if at least half of the members are present. In the idea to compensate any unforeseen absence but to remain a quorum of at least three members, any committee has to consist of at least five members. If you have, e.g., twelve members in the whole supervisory board, this automatically leads to high correlation of members. Although, Aareal Bank AG has in fact five committees (a technology and innovation committee supports the supervisory board in IT issues) and pays attention to a diverse

composition, actually, in every committee three members are equal to another committee. Hence, these persons demonstrate the majority in two committees. As a result, the transposition of this provision would be impossible to comply for Aareal Bank AG.

Independence of members

The independence of members of the management body is treated in the ESMA/EBA paper on suitability, title V no. 18 and we do reference to our comments there. We only would like to emphasise that there is a high urgency to determine that representatives of employees like in the German company system have to be assessed as independent. The draft ESMA/EBA-paper states in para 123 that employees of any entity within the scope of consolidation are not independent. They do not treat the special topic, if this should also include representatives of employees subject to specific security rules like in Germany which ensure their independence.

Especially in regard of provisions like para 42 and para 44, committees should be composed of a sufficient number of independent members and each committees' chair should be independent. (Especially the German) Institutions need a clear provision how to assess their representatives of employees. If they have not been assessed as independent, these members would be excluded from becoming a committee's chair.

Furthermore, please recall that supervisory boards of institutions with more than 2,000 employees in Germany have to be composed by 50 percent of employees' representatives. To have a majority of independent members in committees as required by para 42 and 45 means to strengthen in fact the influence of shareholder representatives. Indeed, representatives of employees represent half of the supervisory board members but would have no particular role within a committee and therefore loose influence on the preparation of the supervisory board decision, respectively on specific competences of a committee which has not to be forwarded to the supervisory board, such as the pre approval of non-auditing services, s. art 5 para 4 of the audit EU regulation No. 2014/537/EC. This is against the idea of a parity voting.

Rotation of memberships

According to para 44 institutions should consider the occasional rotation of chairs and members of committees. As set out in the drafts of the ESMA/EBA paper on suitability, para 16 b. ii., and the ECB guide, page 22, this should trigger a new fit & proper assessment. Combining this with the idea of

mandatory ex-ante assessments before a new member could be appointed, ESMA/EBA paper on suitability, para 166, any motivation for a rotation of memberships is reduced. The documentation efforts and time for ex-ante assessments are not incommensurate the (less) benefits of rotations.

Nevertheless, in our position paper on the ESMA/EBA-paper we deny the necessity of fit & proper tests due to changes (“only”) within the supervisory function as like rotations. Except for the supervisory function’s and the audit committee’s chair, the suitability requirements for the other members are almost similar. This is why we argue that such changes should not cause new fit & proper tests.

Expertise of members

Para 43 requires “expertise” beside to have sufficient knowledge, skills and experience. Neither art 88(2)(1) CRD IV nor the ESMA/EBA guidelines requires more than knowledge, skills and experience which is why it is unclear what the term “expertise” demands. We ask EBA to correct this.

Doubling of duties of committees

There are several provisions determining tasks to more than one committee – this is an entire new approach. We don’t understand how such doubling of responsibilities should contribute to a clear division of duties. To the opposite, in our opinion, it disrupts a well-functioning common system where the supervisory board delegates the preparation of decisions to one committee. By concerning more than this one committee the intention of delegation loses its benefits, since – e.g. in the situation of a supervisory board composed of twelve members – probably three quarter of the members have already decided about such issues, before it is forwarded to the plenary meeting of the supervisory board. Therefore, we ask EBA, to reduce para 24i to the audit committee and not to involve the risk committee in the development and monitoring of the audit plan in addition.

Furthermore, we ask EBA to reduce the provisions as set out in para 46 to the risk committee, since we do not understand why the nomination committee should decide on risk issues, periodically review and decide on the content and frequency of the information on risk reported to them and receiving regular reporting and ad-hoc information concerning the risk profile, risk culture etc. We assume, this was a mistake, because the tasks of a committee have to correspond to the required member’s knowledge, skills and experience. However, according to para 43 from EBA’s view the

nomination committee (only) have to possess qualifications in terms of selection processes, suitability and control practices.

IV. Rules for the risk committee

Information on any breaches in risk issues

According to para 46b the risk committee (we assume that the mentioning of nomination committee is a mistake as explained above) should receive ad-hoc and regular information about the risk profile, risk culture and risk limits and of any breaches that may have occurred and detailed information on and recommendations for corrective measures taken, to be taken or suggested to address them.

The provision is very generic which is why we suggest to clarify what has to be mentioned within the regular reporting and any ad-hoc information in regard of breaches of risk limits. In the regular reporting risk limits and their current levels are illustrated and commented if necessary. This included the potential development of risk limit usage. Ad-hoc information is currently only mandatory if there are material, risk-relevant breaches.

Ensuring the proper involvement of internal and external advice

According to para 46d and 47e the risk committee has to ensure the proper involvement of the internal control functions, other relevant functions and, where necessary, seek external expert advice and has to review the proposed appointment of external consultants that the supervisory function may decide to engage for advice or support.

We don't understand the idea of an overall responsibility of the risk committee for the governance of internal and external advice, regardless of the issue. The risk committee is responsible for risk issues and should therefore be restricted to such. Furthermore, the supervisory board in a whole is according to para 24g only responsible to ensure that the heads of internal control functions are able to act independently [we have already commented on the following direct reporting rights of the internal control functions] and is not responsible to ensure the proper involvement and especially not above mentioned extension to every internal function. Any matter, which is not in the scope of supervisory board's duties could not be delegated and we don't see any reason why this should be a specific, single duty of the risk committee.

In addition, any committees' members and the members of the management body in its supervisory function have to review the appointment of any external consultant itself. Why should for example the risk committee review an external advice on the effectiveness of the risk management framework given to the audit committee? In this case, only the audit committee is capable to review it. Moreover, why should the risk committee review the advice of an external service provider for the annual assessment of suitability, when this is up to the nomination committee? In the idea of a clear division of tasks, this duty has to remain at the relevant and responsible committee.

Examining the alignment between all financial products and services

Pursuant to para 47g the risk committee should 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. The risk committee should 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.

Such a wide scope of monitoring is almost impossible to fulfil. Financial products and services are tailored to the specific needs of the clients and might be of enormous variety. The management of such risks have to be considered in the risk management framework, from a general approach, and the management, assessment and monitoring of this risks are duty of the business lines as first line of defence.

Therefore, we ask EBA to stay within the scope of art. 76(3)(3) CRD IV. Thus, the risk committee shall review whether prices of liabilities and assets offered to clients take fully into account the institution's business model and risk strategy. Where prices do not properly reflect risks in accordance with the business model and risk strategy, the risk committee shall present a remedy plan to the management body.

V. Rules in regard of complex structures, non-standard or non-transparent activities

Para 63 ff., 68 avoiding setting up complex and potentially non-transparent structures

The para 63 ff. put institutions under the general suspicion being intended to set up structures to enable money laundering or financial crimes. This is why para 66 requires to document decisions about structures and being able to justify their decision. This means to document that the catalogue in para 63 is not applicable and the "clear economic rationale or legal purpose" pursuant to para 64,

the understanding of the management body according to para 65 and the policies in place to manage any risks relating to it, para 67, 68.

However, set up structures to enable money laundering or financial crimes is an offence and could be penalised which is why institutions are already have controls and mechanisms in place to prevent that such structures could be implemented within the institution or group. We do not understand to which rational EBA is of the opinion that more provisions and especially an enormous increase of documentation, as set out in the first subparagraph, could be useful.

Moreover, how should an institution analyse the client's intention to set up a particular structure, last sentence of para 68? If a client is intended to set it up for money laundering or financial crimes, he would not state that when the institution asks for it.

Hence, we would like EBA to delete the last sentence of para 68 and para 66 entirely. There is need justifying the documentation efforts.

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

I. Internal governance policy

The introduction of an internal governance policy for an overview about the corresponding framework

According to para 70 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 taking into account the aspects set out in Annex 1 (e.g. composition, selection criteria, number, length of mandate, rotation, age, internal divisions of task; key function holders; description of each functioning of the internal control framework, including its organisation resources, stature, authority; weaknesses identified by each internal control functions and measures taken to address them; operational structure; range of products; geographical scope of business; branches; code of conduct and behaviour).

The provided content for the internal governance policy is nothing new. It is intended as a central document that gives an overview about all internal governance arrangements. We acknowledge the benefit of such a central document which is in Germany at least in line with the requirements to set out requirements for the operational and organisational structure. We would like to emphasise that monitoring more and more documents with equal or similar content increases the administrative work load and at the same time the risk of discrepancies between the different documents which may ultimately lead to operational risks to materialize.

In addition, we deem that this should be a duty of the management body in its management function because the supervisory function in its German corporate governance role is not in charge of developing the policy but to monitor its implementation.

For further comments on para 72 and the conflict with the three-lines-of-defence model, please see our answer to Q6.

II. Rules for corporate values and code of conduct

Definition of acceptable and unacceptable behaviours

According to para 87c the management body should define acceptable and unacceptable behaviours linked in particular to financial misreporting and misconduct, economic and financial crime, including fraud, money laundering and anti-trust practices, financial sanctions, bribery and corruption, market manipulation, mis-selling and other violations of consumer protection laws.

We would like EBA to delete this provision, because it is not possible to reflect any criminal behaviour as unacceptable behaviour in one policy / code of conduct. This would expand the document to an extent not readable for any one. It is suitable to explain all the above mentioned principles and provisions by reference to comprehensive examples. This argument counts for acceptable behaviour vice-versa.

In addition, there are already legal provisions that need no repetitive in institutions internal guidelines.

Q5: Are the guidelines in Title III regarding the principle of proportionality appropriate and sufficiently clear? When providing your answer please specify which aspects and the reasons why. In this respect, institutions are asked to provide quantitative and qualitative information about the size, internal organization and the nature, scale and complexity of the activities of their institution to support their answers.

We appreciate the approach of the European Authority to make requirements more flexible, taking into account the specific situation of an institution or group. We would like to point out that there are several definitions for significance or materiality of institutions for different regulations. We deem a central definition as useful for further harmonizing the requirements to be fulfilled by all banks and would assume that depending on the assessment of the authorities on the specific institution requirements that apply only to large and complex banks should be highlighted. This is a key part in order to make sure that a level playing field is ensured.

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

I. Rules for all internal control functions

Inconsistencies with the three lines of defence-model

Our following comments concern the risk management, the compliance as well as the internal audit function. Their duties are intended to get expanded by – in our opinion – violating the three lines of defence-model.

In this model the first line of defence, the business lines, have to analyse, identify and manage risks on a day-to-day basis (as set out in para 83, 153 and as set out in the corporate governance principles for banks, para 40). Pursuant to para 41 and 42 of the corporate governance principles for banks the RMF as well as the CF are in second line of the model and have to monitor the conduct and treatment of risks and to monitor the compliance with laws, corporate governance rules, regulations, codes and policies to which the bank is subject. The IAF as third line of defence has to control the internal control framework, including the RMF and CF.

Therefore, the internal control function's staff does not perform any monitored operational tasks (para 125a), i.e. should be independent from them (para 152, 176, 184), and should possess sufficient knowledge, skills and experience on their duties (para 151, 177). While the business lines have to identify and manage the risks in their daily work, RMF and CF have to develop and implement control systems and frameworks to monitor their behaviour and IAF overviews this interaction.

However, there are some provisions expanding these defined roles against the three lines of defence model. According to para 161 the RMF should ensure that all risks are identified, assessed, measured, monitored, managed, mitigated and properly reported, although, the identification and managing of risks is up to the business line directly exposed to them. The RMF should only be responsible for a suitable identification process (para 149) and this, taking the proportionate principle into account, only for the material risks (as only required by para 113 of the corporate governance principles for banks). Hence, in the current EBA guidelines from 2011, no. 25.2, the risk control function has only to "ensure each key risk is identified [by the business lines]". Especially in a group context, identification of all risks by only one function is almost impossible. Para 161 does not provide a duty of the RMF but the objective of the risk management framework.

Vice-versa, according to para 72 the CF should analyse how the internal governance policy affects the institution's compliance with legislation, regulation and internal policies. The internal governance policy consists of descriptions of any material control mechanism in place as well as of the organisational structure and in addition the composition and functioning of the management body. As a result, the CF has to control all internal control frameworks whether or not they are compliant. By following this provision, CF would control the IAF as part of the internal control mechanisms, which means that the second line has to control the third line of defence. In addition, this is already assigned to the duties of the IAF, para 185 ff.

By taking this into account, we would like to ask EBA to adjust the following paragraphs: 72, 153, 154, 161, 164.

For our comments on the direct reporting rights to the management board in its supervisory function and direct accountability of IAF, please see our answers to Q2.

II. Rules for the RMF

The extension to future risks

We do not understand what is meant in para 130 by future risks? Any risk is prospective this is what it separates from already occurred damages. Perhaps, EBA could elaborate on this term.

Control of external behaviour

According to para 170 institutions should take appropriate actions against internal or external fraudulent behaviour and breaches of discipline (e.g. breach of internal procedures, breach of limits).

We would like to suggest to specify this provision to address only internal actions and behaviours, since an institution is responsible for its own compliance not for the compliance of third parties. Where third parties act in fraudulent manner which are directed to the respective institution, institutions clearly need to take appropriate defence actions and / or must monitor and report those fraud cases to the respective authorities. Furthermore, this should not be a duty of the RMF but of the CF which is charge of such issues.

III. Rules for the CF

CF's role in the new product approval policy (NPAP)

Pursuant to para 144, 145 CF should be responsible for ensuring internal compliance with the NPAP, including a systematic prior assessment and approval by the CF, including a written opinion from the head of compliance or a person duly authorised by the head of compliance for new products or significant changes to existing products [, processes and systems].

We understand that the confirmation must be documented but would like EBA to take the provision in para 181 as sufficient. According to that, the CF should 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. Any exceeding obligation of further systematic mechanism – as set out in para 144, 145 – is not necessary.

In addition, to ensure internal compliance is not task of the CF but of the business lines which have follow this policies. In the three lines of defence-model the CF is only responsible for the

development of according control systems and the monitoring of compliance (the compliance framework) but could not ensure it.

III. Rules for the IAF

Reporting to the risk committee

The head of the IAF should be able to report directly where appropriate on his own initiative to the management body in its management function of the non-implementation of the corrective measures decided on. This should not prevent him to report, where relevant, to the risk committee.

EBA might primarily mean the audit committee which is the typical addressee of audit committee's reports. Nevertheless, there are reasonable grounds to report the risk committee, in particular in case of findings concerning the risk management framework. We suggest to clarify that the audit committee is the primary addressee and to compliment it afterwards with "this should not prevent him to report where relevant to the risk committee".

The group wide review of all activities and units

According to para 185 the IAF should independently review the compliance of all activities and units of an institution including outsourced activities with institution's policies and procedures and that should ensure that each entity within the group fall within the scope of the IAF.

We would like EBA to consider the proportionality principle, in order to reduce this provision to all material activities and units, outsourced activities as well as each material entity in the group. The overall application is something possible to a framework but not to a function. No function is able to review any activity of any employee in any unit.

IV. Rules for the business continuity management

We ask EBA to take into account that the Basel Committee for Banking Supervision is intended to abolish the "AMA-provisions", para 196.

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


We have no comments on this question.

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?

We have no comments on this section.

Yours sincerely,

Aareal Bank AG


Dr. Eberhard Kriener


Holger Lehnen