27/01/2017

European Banking Authority

Draft Guidelines on internal governance

The Swedish Bankers´ Association, SBA, appreciates the opportunity to comment upon the draft guidelines on internal governance, the "draft guidelines". We support the answer from the European Banking Federation, notably as concerns the difficulties that arise when the guidelines are to be applied in member states with unitary board structures such as Sweden and would like to add the following.

The SBA acknowledges the EBA´s effort to create a more harmonized base for effective arrangements, processes and mechanism of internal governance in financial institutions. However, even if there is an analysis of the potential costs accompanied to the draft guidelines we can see no survey or analysis of the actual need for revising the current guidelines. The current guidelines was based on the finding of the CEBS´s survey as a follow up to the financial crisis in 2008. As stated in the background information to GL44, weak internal governance issues were not identified as a direct trigger for the financial crisis rather insufficient implementation of existing guidelines. In order to take into account weaknesses identified the current guidelines were issued. To be able to achieve public support, understanding and thus focus on the thing that really needs to be done, new requirements should rely on evidence. Even though the directive 2013/36/EU, stipulates that the EBA shall issue guidelines on the arrangements, processes and mechanisms referred to in paragraph 1 (in accordance with paragraph 2) of article 74 of the directive, we believe that the need for, and the scope of new requirements should be carefully analyzed in advance. We are not aware of what, if any, perceived deficiencies in GL44 that have had consequences that merit a complete revision of the guidelines and the consultation document does not shed light on whether any such deficiencies have been identified. The understanding of the guidelines and a proper implementation requires a well-defined rationale and a description of the material changes and the purpose for these. In this context it should also be noticed that some but not all of the explanatory notes in GL 44 have been elevated to requirements in the guidelines without being revised and therefore perceived as deviant.

Besök (Visit):
Blasieholmsgatan 4B
Stockholm
Sverige (Sweden)

Post:
Box 7603
SE-103 94 Stockholm
Sverige (Sweden)

t: +46 (0)8 453 44 00
f: +46 (0)8 796 93 95
e: info@swedishbankers.se
www.swedishbankers.se

It is also difficult to see or discover where changes has been made because the structure has also been changed. A comparison table would be desirable. In some cases just one word has been changed compared to GL44, and it is unclear if the new wording is meant to change the whole meaning of the requirement or if the scope should be the same, see for example subparagraph 92 d. where "significant" is changed to "material" and subparagraph 106 where "management body shall" is changed to "management body should".

The SBA has understood that EBA has intended to take the BCBS Corporate governance principles for banks and the "three-lines of defence model" into account (see subparagraphs 18 and 20 in the Consultation Paper, page 8). We are positive to this approach. However, we believe that it is important that certain changes as outlined below are made since there is a risk that the concept that the first line of defense is overall responsible for risk management, including internal control[1] could easily be misunderstood given the terminology used in the draft guidelines.

The BCBS Guidelines defines internal control system as

> *"A set of rules and controls governing the bank's organizational and operational structure, including reporting processes, and functions for risk management, compliance and internal audit".*

Subparagraph 114 of the draft guidelines describes this model well. However, other parts of the guidelines are less clear on this.Therefore and to underline more clearly that the first line is responsible for risk management and must also establish internal control systems, the SBA suggests that the second and third line of defense (i.e. Risk Control, Compliance and Internal Audit), when referred to collectively is referred to as "*Independent* Control Functions" (rather than *Internal* Control Functions) to better underline that these functions are part of (and not the entire) internal control system of the institution. Consequently the defined term "Heads of Internal Control Functions" should be changed to "Heads of Independent Control Functions". Also, the "Risk Management Function" should be renamed "Risk Control Function". This is because "Risk Management" shall be performed also in the first line (in accordance with what is stated in subparagraph 20) and not only in a second line function. Risk *Control* is the terminology that should be used for the independent risk control performed in the second line.

In order to make it clear that the concept of internal control which the draft guidelines prescribes is the same as outlined in the BCBS Guidelines, the SBA urges the EBA to apply the principles in subparagraph 114 in all relevant parts of the draft guidelines.

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

Further the SBA believes that the draft guidelines in some parts are too detailed and therefore too restrictive. A fundamental problem is the lack of a clear breakdown of the requirements stipulated for the management body on the different parts of the management and the board in relation to the various corporate structures within the EU. Even though the guidelines do not advocate any particular structure and are intended to embrace all existing governance structures it appears to miss the aim to create a guidance that easily can be applied to all sorts of governance structures. The Swedish corporate governance structure lies somewhere in between the Anglo-American and the continental models in several respects. In Sweden the companies act stipulates that companies must have three decision-making bodies in a hierarchical relationship to one another: the shareholders´ meeting, the board of directors and the chief executive officer. In practice the CEO usually carries out some of his duties through delegation to a member of a management team. There must also be a controlling body, the statutory auditor, which is appointed by the shareholders´ meeting. According to the Swedish Corporate Governance Code (which is part of the self-regulation system and applicable to all companies whose shares or depositary receipts are listed on a regulated market in Sweden) the shareholders´ meeting´s decisions on election and remuneration of the board of directors are to be prepared in a structured, clearly stated process governed by the shareholders (through the nomination committee) that provides conditions for well-informed decision-making. The task of the nomination committee is among others to specify the duties and profile of directors, including the chairman, appropriate to the company's operations and in line with the articles of association of the company and the interest of all shareholders. If the shareholders decide to appoint a nomination committee, the committee constitutes a body under the Shareholder´s Meeting.

The EBA stated at the hearing on the 5th of January 2017 that they have chosen to be vague, e.g. such as by not defining the word "management body", with the intention to allow for national authorities to incorporate the requirements in accordance with national law. It would be commendable if this could be expressed in the guidelines.

Answers to the EBA questions

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

The definitions are not clear enough.

- Risk capacity is a new concept defined without any rationale or purpose and it is just mentioned a few times in the guideline. In subparagraph 83 it is used as interchangeable with risk appetite which is not correct and in

subparagraph 84 b. the requirement for all staff to know and understand the risk capacity is too-far reaching.

- The meaning of "staff " could be better defined. Should e.g. contractors be included in the concept? Additionally, the scope of the definition of staff should be amended to reflect the scope of CRR/CRDIV, i.e. delete references to subsidiaries not subject to prudential regulation.
- For reasons stated above, the term *Independent* Control Functions" (rather than *Internal* Control Functions) should be used. Consequently the defined term "Heads of Internal Control Functions" should be changed to "Heads of Independent Control Functions".
- The definition of "Conflict of interest" does not correspond to the use of the concept in the text, subparagraph 9.3.
- The concept of conduct risk should be defined in accordance with EBA/GL/2014/13 – "Conduct risk means the current or prospective risk of losses to an institution arising from inappropriate supply of financial services including cases of wilful or negligent misconduct".
- The definition of Compliance risk in GL44 is not included in the draft guideline and there is no explanation for this. It could be useful with a definition but the one provided for in GL44 is too wide since it includes violations and non-compliance with agreements.
- To increase the understanding it is better to writhe out the meaning of key concepts rather than refer to directives and other documents.

Even though the draft guidelines do not advocate any particular structure and are intended to embrace all existing governance structures it appears to miss the aim to create guidance that easily can be applied to all sorts of governance structures. A conversion clause is not enough to give a clear and sufficient guidance for Member states which do not have a dual board structure as for example Sweden with a kind of unitary board structure (subparagraph 9).

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?

Subparagraph 17 and 19 conflicts with national law. According to the Swedish law there is only one management body that has the responsibility which the guidelines distribute between the management body in its management function and in its supervisory function. It should also be noted that the management body, pursuant to Swedish law, has only a limited executive role which makes it even more difficult to reconcile the dual structure presupposed in the guidelines with how Swedish institutions function in accordance with Swedish law requirements. The responsibilities for the management body according to Swedish law may however be

documented and duly approved. Further, it is unclear whether the requirement in subparagraph 19 h. aiming at the management body or the committees. The Swedish law does not require the management body to include notes of the discussion in the minutes of the meeting. Rather, from the viewpoint of applicable Swedish law the minutes is intended to provide information about decisions taken and any dissenting opinions. A requirement to minute the management body´s discussion into the minutes is a far-reaching requirement that is hard to reconcile with the purpose of the minutes pursuant to Swedish law. Moreover, a requirement to include minutes of the discussion would most likely prevent and hamper the possibility for discussion between the members of the management body. Thus, both legal aspects and considerations of efficiency – namely, how best to achieve substantial and free discussions in the management body – can be invoked as arguments against requiring minuets to be included in the minutes. It should be sufficient to document the decision taken. In order to encourage the ambition that the discussion in the management body shall be open and critical (as outlined e.g. in subparagraph 26), the SBA suggests that the wording in subparagraph 19 h which suggesting that also discussions should be recorded is taken out in the final version of the guidelines.

Furthermore, the management body in its supervisory form is required to set the strategy of the institutions. Nonetheless, it is also proposed (in subparagraph 23) to be responsible for challenging said strategy. This seems redundant and somewhat difficult to achieve.

Notwithstanding the abovementioned conflict to Swedish legislation, through the proposal the EBA attached existing terminology, such as *monitor* (in the consultation associated with day-to-day 2nd line activities) and *review* (associated with Internal Audit mandate), to the activities of the management body in its supervisory function. For consistency and to ease interpretation of the final guidelines, it should be preferred to use the term "*ensure"*, i.e. the management body ensures that the activity in question takes place. This would also reflect the actual activities of the management body in its supervisory function better. Subparagraph 23 should therefore be changed as follow:

"The management body in its supervisory function should challenge management actions and decisions and perform their role independently from the management body in its management function. The management body in its supervisory function should ensure the performance of the management body in its management function and that the institution's strategy and objectives are implemented in line with the strategy and objectives that have been defined and approved by the former. 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."

Based on experiences from Sweden, where the Swedish Code of Corporate Governance contains a rule stating that no more than one member of the board may be a member of the executive management of the company, the SBA would recommend not to include the part of subparagraph 24 a) regarding that no members of the management body in its supervisory function may perform an executive function in the final wording of the guidelines, but rather either let this be a matter regulated in national law/regulations or to accept that at least one member of the management body in its supervisory function also holds an executive function.

In subparagraph 24 i) the risk committee is included. It should be enough that the audit committee is involved.

In subparagraph 26 it is stated that the chair should encourage and promote open and critical discussions. A requirement to add the minutes of the discussion to the minutes is likely to counteract an open and critical discussion, see also above.

Subparagraph 32 is an example where the conversion clause does not work. According to Swedish law the "management body in its management function" and the "management body" in some cases must be interpreted as the CEO. The CEO shall as such make decisions as provided for by law as well as in accordance with the delegation from the management body. Due to this the last sentence in the subparagraph should be deleted.

In the explanatory note on page 19-20, second paragraph, there is an explanation on how the 1-tier structure works which is not in conformity with the statement in the beginning of the draft guidelines where it says that the CEO is part of the management body in its management function.

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

As stated above a conversion clause is neither appropriate nor sufficiently clear to cover all management structures among the Member States.

The requirement to create different specialised committees with independent members require very large boards which may counteract efficiency and rather create a diffuse and ineffective work within the management body. The requirements in the guidelines on suitability may also counteract the possibility to keep a very large and suitable management at all times for both large and small entities. This covers also subparagraph 42. Overall the requirements on the different committees are too detailed, it must be possible to structure the business in different ways depending on the national law and the business in each entity.

Further, the rationale behind the requirement is weak, at least in relation to Swedish law. According to Swedish regulations a unitary board, which has collective responsibility, shall/may establish various committees consisting of board members. The committees produce data and suggestions that are discussed and decides by the board collectively.

It is not possible according to Swedish law to create a nomination committee with members from the management board.

Subparagraph 47 tasks the Risk Committee with a set list of activities. While these activities are relevant, it should be allowed for the Risk Committee to look into items outside the scope of this list from a risk perspective. Therefore it should be preferable to make the list open ended.

Moreover, subparagraph 47 grants the Risk Committee with the mandate to review the proposed appointment of external consultants by board. While it remains unclear what this review exactly entails in terms of veto rights, this proposal could be considered out of sync with proper governance, as it would allow a subgroup of the board to force the hand of the majority of the highest ranking body in the institution (between annual shareholders assemblies).

Furthermore, it is essential to keep a clear line between the role of the risk committee and the control function. The overall responsibility for the risk committee is normally to create policies and ensure the compliance with those. The risk control function normally has the responsibility to control the compliance further down in the organisations. It is important to keep the boundary between different functions within the entity. The last sentence of subparagraph 47 g. should be changed as follows:

The risk committee should assess the risks associated with the offered financial products and services and examine the alignment with the ~~prices assigned and profit gained from~~ institutions liabilities and assets relative to those products and services.

The word quality in subparagraph 50 a. should be removed “monitor the effectiveness of the institution´s internal ~~quality~~ control and risk management systems and, where applicable, its internal audit, regarding the financial reporting of the audited institution:”.

The SBA also suggests that it is, in subparagraph 50 h, clarified that the duty to review audit reports is limited to such audit reports that are submitted to the audit committee. This would imply that the new wording of 50 h would be “review audit reports *that are submitted to the audit committee”.*

Subparagraph 45 and 50 specify the requirements on the members of the audit committee and the role the committee has. In directive 2006/43/EU (amended by directive 2014/56/EU article 1 subparagraph 32 – Chapter X Audit Committee) there are requirements regarding the formation and function of an audit committee with equal content. The SBA can see no reason to duplicate the requirements in the draft guidelines. Thus, these subparagraphs should be deleted.

Regarding subparagraph 63 it is unclear what is meant with "structures".

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

The criteria in Annex I is unclear and it also unclear how the requirements are to be applied in practice. What a policy should contain have been mixed with actions taken or shortcomings noted by control functions. It is not reasonable to require a policy to include e.g. weaknesses identified by each control function (6 c) or recommendations made by the internal audit function (6 d). Even though recommendations by the control functions should be considered, these should not be included in a policy document. Annex I should therefore be rewritten.

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

Subparagraph 74 should be coordinated with the Guidelines on supervisory review process. The supervisory authority has the possibility to require any information from the entity when the authority so wishes. Due to this the requirement to communicate the policy with the competent authority should be deleted unless there is a justified purpose for the requirement.

Subparagraph 75 should be amended to include mixed financial holding companies and financial holding companies in the scope. According to article 109 in CRD IV parent undertakings and subsidiaries are obliged to fulfil governance requirements on group level. Parent undertakings include the mentioned holding companies.

Leaving those holding companies out of the scope on group level causes conflicts in relation to article 109 CRD IV, article 246 Solvency II, article 7.1 BRRD and Swedish law. The term "parent undertaking", as used in article 109 CRD IV should be used in the guidelines as well.

Additionally, in subparagraph 75 the EBA interpret the scope of the guidelines to include banking group subsidiaries outside the scope of the CRD IV. The SBA considers this to potentially conflict with the mandate granted to the EBA in CRD IV, but also in conflict with the purpose. Common to entities in the scope of the CRD IV are that they affect the surrounding society in a way that requires a stronger insight into their stability and survival. Conversely, if a subsidiary is not included in the scope of the CRDIV there would not be a presumption for an impact on the surrounding society. The same approach should be applied regarding the additional requirement on governance in the draft guidelines. Subparagraph 75 should therefore be changes as follows:

In accordance with Article 109 of Directive 2013/36/EU, the consolidating institution should ensure that governance arrangements, processes and mechanisms are consistent and well integrated on a consolidated and sub consolidated basis. To this end all subsidiaries within the scope of prudential consolidation, ***ex****~~in~~cluding those not subject to Directive 2013/36/EU, should implement such arrangements, processes and mechanisms. […]*

Subparagraph 76, it should not be the authority´s task to ensure that a group-wide written internal governance policy is compliant with the requirement but rather the consolidating institution. The authority should review the compliance and take actions if necessary. The first sentence should be change "… and competent authority should review that …"

Regarding risk culture there could be some guidance on what a following-up procedure or monitoring procedure should include.

Subparagraph 84 a. stipulates that staff should act in accordance with all applicable laws and regulation and promptly escalate observe non-compliance within or outside the institutions. It is unclear what is meant with outside the institution. This must be explained. The difference in scope or severity in subparagraph 84 a. (promptly escalate), subparagraph 96-103 (internal alert procedure) and subparagraph 99 (whistle blowing) should be developed.

Subparagraph 87 c. the requirement to list unacceptable behaviours in a policy is not possible. It may result in a list of black or white behaviour, if an unacceptable behaviour is not on the list it can be interpreted as an accepted behaviour. Normally the law and regulations specifies what is unacceptable behaviour and it should be

enough to give some examples, if any, of unacceptable behaviours. Further, it would be very difficult to review the compliance of the code of conduct relative a black and white list.

According to subparagraph 88 an institution should defined the function responsible for evaluating breaches of the code of conduct. Further, in subparagraph 89 it states that a regular review of the implementation and compliance with those ethical and professional standards should be performed. It seems as if these two requirements governing the same thing or, is the intention that the function referred to in subparagraph 88 regularly should be review in accordance with subparagraph 89? This must be clarified. Furthermore, it should be sufficient to send reports on deviations to the management body and on annual basis a report on how the implementation and compliance with ethical and professional standards are performed.

The wording in subparagraph 91 about conflicts of interests is unclear regarding the meaning of institutional protection scheme. Conflicts of interests is well described in GL 44 subparagraph 16.2 and this wording, also including customers, should be retained.

The amended requirement in subparagraph 92 f. leads to a requirement to review all legal and natural persons who may have a relation to persons under (a) to (e) which seems very far-fetching. The requirement should be deleted.

The requirement in subparagraph 95 to issue a statement – if any conflict of interest is identified – may violate the bank secrecy and should therefore be removed if the requirement refer to a public publishing. The meaning of "issue a statement" should be clarified. Anonymised or information on a generally basis may be published.

The requirement in subparagraph 97 should not prevent staff to report to their manager/head. It is important to clarify the purpose with an internal alert procedure and the requirement to report an incident. The overall aim must be that incidents actually are reported. Further, an internal alert procedure should not be mixed with a whistle blowing system.

The last part of subparagraph 102 b. is unclear and should be removed "… in the context of further investigations or subsequent judicial proceedings …". Further, the requirement in subparagraph 102 d. is not compatible with the possibility to be anonymous.

Subparagraph 109 states that the policy should cover intragroup outsourcing and give as an example outsourcing by a separate legal entity within an institution´s group. The wording "e.g." should be changed to i.e.

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

The part on proportionality should be placed at the beginning of the guidelines since it covers the whole guidelines.

Further, the part on proportionality only refers to institutions. Institutions is defined as credit institutions and investments firms. It should be clarified how the proportionality principle relates to other entities in a consolidating situations.

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

The guidelines in Title IV regarding the internal control framework are not sufficiently clear. The Risk Control Function in GL 44 has in the draft guidelines been renamed to Risk Management Function, although the responsibilities appear to equate to those in GL 44. The EBA should clarify what the change of terminology indicates in terms of changes as to the overall responsibilities of the function.

The wording "strong" in subparagraph 113 should be clarified.

Subparagraph 119 is one example where it is not specified which function is responsible and can be interpreted as together. It could be clarified by adding "in their respective area of responsibility".

The requirements in subparagraph 121 is not compatible with Swedish law since a board member never could have an executive responsibility, except for the CEO when he/she is part of the board. Further, if the CEO should be responsible for an internal control function, it is impossible for that person to be independent (see also subparagraph 125 b.). Similarly, it is in not feasible for the RMF and compliance functions to be completely independent from the management body whom they monitor, as the management body is responsible for overseeing also the internal control functions, cf. subparagraph 116. We would therefore suggest rephrasing subparagraph 125 as follows:

"In order for the internal control functions to be regarded as independent the following conditions should be met, notwithstanding the responsibility of members of the management body:

a. *[..]*
b. *[..]*

c. *the head of an internal control function is not subordinate to a person who has responsibility for managing the activities the internal control function monitors and controls; and*
d. *[..]*

Subparagraph 128 states that the head of the internal control function etc. are still responsible for these activities and for maintaining an internal control function within the institution. If an institution outsource the operational task of the internal control function, the institution should not have to maintain this function within the institution but rather to maintain the ability to verify and control that the outsourced activities are properly managed. Further, the principle of proportionality has to be taken into account.

In subparagraph 129 the concept of internal control functions and institutions are mixed. The paragraph should be rewritten.

Subparagraph 130 and 132 seems to regulate the same issues and should as such be assembled to increase the understanding and readability.

In GL 44 it is stipulated that an institution should have a risk management framework and an internal control framework. The draft guidelines, although including largely the same features as previously for these two, depicts the risk management framework as a subset of the internal control framework (subparagraph 130). It would be beneficial if the EBA would clarify the interaction between the risk management framework and the internal control framework, as well as the roles and responsibilities of the parties involved.

It would be beneficial if the EBA would clarify what is meant with controls (as in subparagraph 131) and clarify the link to the internal control framework.

In subparagraph 134, the EBA provides that the risk management framework shall be *"subject to independent internal review … taking into account information from Risk Management Function".* As per subparagraph 19, management body is responsible for setting, approving and overseeing risk management framework, in paragraph 130, it is made clear that the risk management framework shall be holistic across all business lines, internal units, and internal control functions. In subparagraph 22 (background), RMF should be involved in the setting of the framework too.

EBA should elaborate on which function in the institution is appropriate to conduct the independent internal review of the risk management framework, whether this is meant solely for the independent audit function, or if the risk management function ought to perform review independent from its involvement in setting the framework.

The example in subparagraph 137, last sentence, does not seem to belong in this guidelines since it is regulated in the CRD IV. The example fits better in an explanatory note in the same way as in GL44. The same applies to the example in subparagraph 138, which should be placed in an explanatory note or removed.

In subparagraph 144 and 145 the responsibility for ensuring internal compliance with the new product approval policy has been shared between the compliance function and the risk management function. A shared responsibility risk creating either overlap or that issues fall in-between. An institution should be able to assign the main responsibility to either one of the functions, risk or compliance, see also subparagraph 148. Further, it would be desirable if all the requirement regarding the new product process could be subsumed under the same chapter, see for example subparagraph 158-160 regarding risk and 181 regarding compliance.

Further, the wording in subparagraph 145 seems to give the compliance function veto "… and approval by the compliance function". The compliance function should assess compliance with the new product and significant changes procedure and submit a written opinion, but the compliance function should not have veto.

In subparagraph 149 the risk management function (RMF) is discussed. The text is difficult to understand and apply since it does not take into consideration the different lines of defence nor the responsibility which lies whit the business, first line. This ought to be clarified by the EBA.

Regarding subparagraph 158 the text could be more flexible and therefore changed as follows.

In line with section 14, before decisions on material changes or exceptional transactions are taken, the RMF should be involved, <u>when relevant,</u> in the evaluation of the impact of such changes and exceptional transactions on the institution´s and group´s overall risk and should report its finding directly to the <u>appropriate</u> management ~~body~~ <u>level</u> before a decision on the change is taken.

In subparagraph 160 different kind of situations seems to have been mixed without any real logic. A catch-all paragraph. The paragraph should be change to an explanatory note.

In the first sentence in subparagraph 175, "to manage its compliance risk", should be changed to, "to monitor its compliance risk".

Subparagraph 178 refers to "system". To clarify that the term system does not necessarily mean an IT-system the term "process" could be used.

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

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

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

The Internal Audit Function is not tasked with monitoring, but is - in subparagraph 183 - nonetheless required to have "monitoring tools". These requirements do not match and should be changed, either by deleting the reference to monitoring tools or by a clarification. The SBA suggests that the third sentence or subparagraph 183 should be change as follows:

In particular, the institution should ensure that qualification of the IAF and its resources, in particular ~~the monitoring tools and~~ the risk analysis methods are in adequacy with its size, locations and the nature, scale and complexity of the risks associated with the institution's model and business activities and risk culture and risk appetite.

In subparagraph 185 it is stated that the IAF should independently review the compliance of all activities and units of an institution including outsourced activities. It should be clarified that the IAF should review the quality of the governance documentation in combination with the procedure and that the institution operates in accordance with internal policies and procedures. It is also within the scope of the internal audit function´s mandate to review outsourced activities and therefore there is no need for further clarification. The SBA suggests that the subparagraph is change as follows:

The IAF should regularly review if the institution~~, including outsourced activities,~~ operates in accordance with internal policies and procedures and that each entity within the group falls within the scope of the IAF. The IAF should also regularly review if all governing policies are fit for purpose and compliant with laws and regulations.

Regarding subparagraph 189 the internal audit function should also have unfettered access to persons within the institute. Accordingly the first sentence should be changed as follows.

"The IAF should have unfettered institution wide access to any persons, records, documents, information and buildings of the institution."

The requirement in subparagraph 192 is not compatible with GL44 subparagraph 29 5. which states that the audit plan should be approved by the audit committee and/or the management body. This should also be stated in this guideline. It is also unclear what is meant by "… on the basis of the annual control objectives…". The IAS 2010.A1 states that "The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process". The fact that the work of the internal audit function should follow a risk based approach is already stated in subparagraph 191. In the light of that subparagraph 192 should be changed as follows.

"An audit plan should be drawn up at least once a year ~~on the basis of the annual control objectives in line with the guidance of the management body in its supervisory function´s~~ and be approved by the audit committee and/or the management body.

The last sentence in subparagraph 193 should be removed. "*All audit recommendations should be subject to a formal follow-up procedure by the respective levels of management to ensure and report their effective and timely resolution. The head of the IAF should be able to report directly where appropriate and on his/her own initiative to the management body in its supervisory function of the non- implementation of the corrective measures decided on. ~~This should not prevent him to report where relevant, to the risk committee."~~*

Subparagraph 196 is incomplete, something is missing. Further, it is unclear if the text refers to the first line or the second line of defence. It is also unclear why the advanced measurement approaches, AMA, is included in the text since the AMA will in the future no longer be applicable.

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

No comment.

SWEDISH BANKERS' ASSOCIATION

Hans Lindberg Åsa Arffman