Baselcommittee@bis.org

Division Bank and Insurance
Austrian Federal Economic Chamber
Wiedner Hauptstraße 63 | P.O. Box 320
1045 Vienna
T +43 (0)5 90 900-ext | F +43 (0)5 90 900-272
E bsbv@wko.at
W http://wko.at/bsbv

Your reference, Your message of	Our reference, contact person	Extension	Date
	BSBV 189/Dr.Priester/Ob	3133	6.3.2012

Response to the Basel Committee on Banking Supervision - The internal audit function in banks - Consultation

Please allow us to respond to the consultative document of the Basel Committee on "the internal audit function in banks" as follows:

1. General

In essence, we support reconciliation with the "International Standards for the Professional Practice of Internal Auditing" (e.g. adoption of the code of ethics).

What we need to point out is that most of the principles relevant to the internal audit function already conform with the usual standards and therefore do not constitute a major innovation.

The close association between internal auditors, supervisory board and supervisor (OeNB, FMA) that is contemplated by this draft needs to be seen critically, since it may jeopardise the foundation for an independent and objective performance of internal auditing obligations.

This independence, but also the organisational integration of internal auditing as a function of management, are aspects of the internal audit function and have been duly enshrined in Austrian law (sec 42 Federal Banking Act ["BWG"]).

The consultative document sets out the principle of good co-operation between external bank supervisors and internal auditors by requiring direct communication and control while eliminating the bank's responsible bodies. In so doing, it pushes beyond what is required by the internationally recognised "International Standards for the Professional Practice of Internal Auditing".

The specific demand to have the audit plan reviewed and approved by the audit committee, too, requires a disproportionately high effort, since, in the current set-up, the audit plan needs to be reviewed and approved by the management board anyway (and also by internal group audit in credit institution groups).

2. Our comments on the individual provisions:

- With reference to principle 1: We would suggest completing the definition of the purpose of Internal Audit (IA) functions to include the goal to enhance the effectiveness of internal control, risk management and governance processes.
  We would suggest giving appropriate emphasis to the consultancy role that IA could perform, in line with the definition of "internal auditing" in the international professional standards issued by IIA.
  What needs to be clarified is whether the term "quality" (concerning a bank's internal control, risk management and governance processes) comprises "adequacy" or "efficiency", or both. We would recommend bringing this in line with the provision under paragraph 59 "*The internal audit function employs a risk-based approach to assess the efficiency and effectiveness of the design and operation of internal control* […]"?
  Paragraph 8: We would suggest putting greater emphasis on the concept involving the "risk-based approach" to determine their respective work plans and actions. This could be highlighted in a dedicated principle, for example, or guidelines could be drawn up that outline the way this kind of approach could be pursued.
  Paragraph 8: With reference to the phrase "*The internal audit function plays a crucial role in the ongoing maintenance and assessment of a bank's internal control*" we would suggest clearly stating that "ongoing maintenance" is the bank management's responsibility.

- With reference to principle 5: We would suggest adding the "responsibilities" of internal audit as a key aspect that needs to be defined in the charter in order to be consistent with the respective paragraphs of the principle.
  Paragraph 23: The sentence "*The charter […] It should be available to all internal and external stakeholders of the organisation*" needs to be clarified to determine whether the purpose is for the bank to give due publicity to its audit charter, e.g. by publishing it on its website?
  Paragraph 24: We would suggest using "must" instead of "should" in "*At a minimum, an internal audit charter should establish: […]*", in accordance with the provision under the IIA International Standards (PA 1000-1).

  Generally, we would like to acknowledge that this approach is inspired by the Anglo-Saxon board system. Although the introduction under paragraph 5 affirms that there is an awareness of the varying structure, the subsequent representations reveal a clear tendency toward "senior management" and "board of directors" (consisting of both executives and non-executives). There is an attempt to factor in the differences between the Anglo-Saxon and Central European corporate charter model through references of analogy; the clearly imputed transferability, however, does not exist. And this gives rise to legal uncertainty. We would therefore recommend providing a clear statement on how the rules put forward are in fact to be implemented under the present system of law (or, generally, in view of the Central European corporate charter model). The consultation paper formally equates concepts such as "senior management" with management board and "board of directors" with supervisory board, although there are material differences

and this gives rise to the present problematic.

- With reference to principle 6: We would suggest adding specific reference to the scope of the parent company's internal audit activities in groups. This should allow an appropriate steering and coordination role along with proper monitoring and control over group risk. We would advise rephrasing the sentence "[…] *The head of internal audit should ensure that all material entities and all material activities of the bank are audited at least once within an appropriate period of time (audit cycle)"*. The rephrasing would be more consistent with the risk-oriented approach stated on page 4, paragraph 8 "*both internal auditors and supervisors use risk based approaches to determine their respective work plans and actions*".

- With reference to principle 7: The envisaged direct reporting to the supervisor will cause the supervisor to impose stipulations and also to take on responsibility for the audit requirements/subjects.

  With reference to the "adequate coverage of regulatory matters", which is consistent with principles defined in other parts of the document (e.g. paragraph 8), our interpretation is that such coverage should be ensured in a risk-based approach perspective.
  Paragraph 30: The same interpretation is given as for the previous bullet (risk-based perspective), making reference to the term "relevant authorities"

- With reference to principle 8: As before, the installation of a permanent or own organisational unit should only be required as of a certain size, especially when it comes to smaller institutions (comparable to the regulations of sec. 42 (6) BWG: € 150 m total assets, average headcount of 30 persons, etc.).

- With reference to principle 9: With regard to paragraph 43, we agree with the recommendation that there should be an independent review of the internal audit function from time to time.
  For complex organisations, Bank Austria believes that a two-tier quality assessment review system (both internally and externally) should be adopted to assess and improve the quality of the service provided by the internal audit function. An internal quality assessment review is performed once every three years, more often in specific cases. The scope of an assessment of the entire spectrum of audit activities (full scope) may vary from that of an assessment of only selected activities or specific areas of activity of local internal auditors. A qualified and independent external team conducts an external quality assessment review at least every five years in line with IIA standards.

  With reference to paragraph 45, we believe that it is vital to provide internal auditors with full knowledge and an overview of the whole business in order for them to perform their duties. Each bank to which the guidance applies should decide the best to implement this based on how it is organized, without prejudicing the independence of internal auditors.

- With reference to principle 10: Generally, we agree with this principle. In Austria, however, the internal audit function is subordinated not to the board of directors but to the management board. Moreover, the audit plan is not approved but only

noted/acknowledged.

Given this reporting line, the points referring to the approval by the board of directors/audit committee would not be applicable for the internal audit function in Austrian banks.

We believe that large and complex financial companies should create a specialized “audit committee” endowed with proposing and consultative functions within the board of directors to cover all control matters that fall into the board of directors' authority.

- With reference to principle 11 - Paragraph 51: Compliance with the "sound internal auditing standards" also comprises evaluating the activities of internal audit every 5 years. In view of smaller institutions, this appears impracticable and inappropriate, since any such requirement would incur additional costs for the banks.

- With reference to principle 11 - Paragraph 52: As a result of this formulation, the audit committee has control over the head of internal audit in terms of his/her personal requirements. However, this would lead to dual subordination, i.e. under the management board and the audit committee (supervisory board), which would prove to be problematic whenever differences between the management board and audit committee arise.

- With reference to principle 12: What needs to be clarified is that only material findings must be communicated to the audit committee and that the main reporting line to the management board must be ensured as before.

- With reference to principle 13: We would suggest defining the responsibilities for audit plan approval more clearly, giving due consideration to the different governance models (one-tier or two-tier).
- With reference to principle 14: We would suggest amending the verb “complement” as otherwise the internal audit function may be expected to assume (and not only assess in line with its actual mission) operational roles in operational management, risk management and compliance activities, which would be at odds with the principles included in paragraph 13 stipulating the support of internal audit’s independence and objectivity.
  Paragraph 59: We would suggest reconsidering the following sentence “*…the assessment of “efficiency” of the design and operation of internal control”* as it seems inconsistent with the definition of internal audit given in paragraph 9, where the evaluation relates to the “effectiveness” of risk management, control and governance processes.

- With reference to principle 14: The internal audit function in a group structure or holding company structure should be established centrally by the parent bank.
  According to sec. 42 BWG “Credit institutions are to set up an internal audit unit”. According to this provision, the responsibility is in fact with the management board. The principle of having the parent bank establish the internal audit function does not allow the management board to abide by the Federal Banking Act (BWG). We would suggest clarifying the meaning of “established centrally by the parent bank”. What needs to be made clear is whether the “establishment” refers to aspects such as the organisation of the internal audit functions in a group perspective, the definition of group common audit methodologies and of the overall budget.

Paragraph 60: In order to support a risk-based approach, also in the organisation of internal audit functions in a group perspective, we would suggest amending the sentence as follows: "*In a group structure […] for ensuring that internal audit policies and mechanism are appropriate to the structure, business activities and risks of all material components of the group*".
Paragraph 61: We would suggest clarifying what is intended by "group's internal audit strategy": e.g. budgets, methodologies, organisational structures, IT tools and staff, risk assessment, audit plans.

- With reference to principle 15: A more precise definition is needed to determine how this is meant, since, by its very nature, the bonus (part of the remuneration) is tied to a company's performance.
  We are referring to principle 2 paragraph 15.

- With reference to principle 16: Greater co-operation/closer relationship to the bank supervisors - paragraphs 69ff: We generally welcome the underlying idea of these rules calling for enhanced communication between the supervisory authorities, but they need to be adapted to take into account the national supervisory structure and architecture as well as the principle of proportionality. The direct (periodic) reporting mentioned in paragraph 71, in particular, is inspired by the Anglo-American "one board system", in which internal audit is located at management level; this runs counter to the regulations under company law in continental European law under which a direct flow of information is inadmissible. National specificities that warrant the flow of information between the supervisor and internal audit in different ways need to be taken into account. In Austria, for instance, the law has been requiring the submission of a mandatory quarterly report to the supervisor since the regulatory reform of 2007; here, the state commissioner is under the authority of the supervisor function.
  The Basel Committee/bank supervisor further needs to clarify what is meant by *"main internal audit findings"* and whether local internal audit can apply its own rules regarding the classification of audit results.

- Paragraph 73: Given the perspective of a risk-based audit approach, which should lead to flexible audit plans, we would suggest the following rephrasing: "*In case of major divergence from the internal audit plan, supervisors should obtain an understanding of the circumstances which led to the changes* […]".

- With reference to principle 17 – paragraph 78: The topics mentioned in (i) through (iii) are primarily subject to the evaluation of the auditor.
  We are referring to principle 16 – paragraph 78.

  We support this principle and consider the assessment of the internal audit function by bank supervisors to be a fundamental step towards contributing to an internal control framework that is suitable for its purpose, including timely and effective reporting and a holistic approach to risk management.
  Paragraph 83: With regard to the introduction of "key internal auditors" for remuneration matters, Bank Austria believes that each bank should identify its key internal auditors on the basis of a self-assessment as provided in Directive 2010/76/EU of 24 November 2010 ("CRD III").
  Paragraph 87: We believe that, stricto sensu, the formal communication of the appointment of a new head of the internal audit (or his/her exit) to the supervisory

authority should be made by the bank's proper functions rather than by the audit committee.
What does “regularly assess” mean? Does it imply an annual formal and specific assessment by means of direct inspection or is it a more general ongoing assessment based on the regular relationships with IA?

- Principle 18: We agree with this principle. We take the view that the supervisory authorities already have the appropriate powers to address the mentioned issues.
- Principle 19: We agree with this principle.
  Paragraph 91: We would like to observe that the assessment of the internal audit function by supervisory authorities will primarily contribute to the overall evaluation of the bank’s internal control system, and secondarily to the bank’s overall risk profile.
- Principle 20: The supervisory authority should be prepared to take informal or formal supervisory actions requiring both the senior management and the board to remedy any identified shortcomings relating to the internal audit function within a specified timeframe and to provide the supervisor with periodic written progress reports.
  Paragraph 94: Are the following sentences supposed to mean the same: “to take informal or formal supervisory action” and “public or non-public nature” (see principle 20)? If not, it would be appropriate to explain or provide examples to clarify this.

- With reference to principle 23: The internal audit function's status should be approved by the board.
- With reference to principle 29: Input to the audit plan is to be provided by the board.
- With reference to principle 49: The audit committee would approve the audit plan and give senior management specifications on how it is to be implemented in a timely manner.
- With reference to paragraph 53: The internal audit function is accountable to the board/audit committee on all matters.
- With reference to paragraph 54: This paragraph distinguishes between "inform senior management“ and "report to the board“. However, "report" is the strongest form of communication and indicates that the internal audit function is assigned to the board. These notions run counter to Austrian legal standards.
  The Austrian Stock Corporation Act (AktG) stipulates that the management board is a company's leading and operative body, while the supervisory board supervises the management board. It is the task of the audit committee to monitor the effectiveness of the internal audit system.
  As a committee of the supervisory board, this body also has a control function.

  Sec. 42 (1) BWG stipulates that internal audit is under the direct authority of the directors, i.e. of the operative body. Sec. 42 (3) BWG further standardises that the internal audit function reports to all directors. Reports on the audit areas and major audit results must be submitted to the chairman of the supervisory board and the audit committee once every quarter.
  These rules indicate that internal audit is an institution that directly reports to the management board; consequently, there is no direct assignment to the supervisory board or audit committee.
  Generally, the tasks of the supervisory authorities, as envisaged by Austrian legislators, i.e. the monitoring of the internal audit system, would be replaced by a stronger, more emphasised control component and the associated operative intervention in internal audit matters.

With the envisaged rights of intervention (Annex 2 lit m-o), the decision-making powers of the management board would be limited in terms of internal auditing. This would cause the relationship between management board and internal audit to be recast. The paper indicates that internal audit is ultimately expected to audit the management and the business strategy (cf. - for lack of any Austrian regulations - the BaFin explanations regarding MaRisk as amended on 15 December 2010, par 1 on AT 4.2 Strategies: The content of the business strategy lies in the sole responsibility of the management and is not subject of any auditing by ... internal audit. ...). Under such circumstances, any co-operation between the management board and internal audit would be impracticable, since internal audit would ultimately be considered a foreign entity in its own company (=instrument of the supervisory board/audit committee/bank supervisor).
The classical internal audit function as an instrument of business management would become obsolete as a result.

The passage "... The principles set out in this document should be applied in accordance with the applicable national corporate governance structure of each country." from paragraph 5 of the introduction provides a means of overcoming the differences.

- **Principle 17-73 - Relationship to bank supervisors**

Paragraphs 71 through 73, in particular, merit some debate, as they provide bank supervisors with various means of intervention. Paragraph 67 specifies that bank supervisors and internal auditors have different roles to play and that independence should not be undermined, but internal auditors are drawn into a conflict of interest nevertheless.
This conflict of interest results since you have the bank supervisors on the one hand and the company's owners and their bodies on the other, each with their own take on things, and internal auditors would be caught between competing interests.

Furthermore, there is the risk that internal audit becomes the extended arm of the bank supervisors, impairing the effectiveness of the company's internal audit function and becoming counterproductive.

The clause under paragraph 5 would have to be applied in order to ensure an adequate interpretation of the paper in compliance with the Austrian law. Otherwise, the Austrian law relating to corporate governance structure would have to be radically amended.
When it comes to the relationship to bank supervisors, the independence of the internal audit function should be given greater emphasis. At any rate, a regular reporting line from internal audit to the bank supervisors appears counterproductive.
Although par. 9 quotes the well-proven IIA definition of the term "internal audit", we need to point out that key tasks of internal audit - i.e. audit of the effectiveness and expediency - clearly take a back seat in the remaining parts of the draft and both legal and risk-oriented topics take centre stage.
To warrant the effectiveness of internal audit, these tasks too would have to be given due consideration in the draft.

If this provision is retained, the Basel Committee/bank supervisors would need to clarify whether local audit should report the audit plan and its amendment/compliance issues to the supervisors automatically or whether the supervisors need to actively request

submission. The formulation is unclear as to whether the audit plan of the coming year is to be submitted to the supervisors before the local internal audit function submits it to the management board for review and approval or not until after review and approval has been given.

- **Annex 2:**
  *) with regard to (i): What needs to be made clear is that not every internal audit report will be transmitted, but only a summary of the major findings and audits.

  *) with regard to (m): this section contains a contradiction, duplicating the work of the remuneration committee, since, pursuant to sec 39b BWG (incl. Annex), the remuneration committee is to be concerned with the instances of control, which, as it happens, include internal audit.

  *) **ISA:** In our view, the International Standards on Auditing may only mandate the auditor to co-operate with internal audit, but they cannot be stipulated as binding standards for internal audit.

Kindly give our remarks due consideration.

Sincerely,

Dr. Herbert Pichler
Division Bank and Insurance