# Comments

## By the German Banking Industry Committee on the Basel Committee on Banking Supervision's Consultative Document

## "The internal audit function in banks"

Basel Committee on Banking Supervision
- via E-Mail: baselcommittee@bis.org -

Contact: Stefan Blömer
National Association of German
Cooperative Banks
Telephone: +49 30 2021-0
Telefax: +49 30 2021-1900
E-Mail: risikoanalyse@bvr.de

Berlin, 12-03-02

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public-sector banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks. Collectively, they represent more than 2,200 banks.

- via E-Mail: baselcommittee@bis.org - - via E-Mail: baselcommittee@bis.org -

Coordinator:
National Association of German
Cooperative Banks
Schellingstraße 4 | 10785 Berlin | Germany
Telephone: +49 30 2021-0
Telefax: +49 30 2021-1900
www.die-deutsche-kreditwirtschaft.de

**Comments "The internal audit function in banks"**

Dear Sir or Madam,

We appreciate the opportunity to share our comments regarding the aforementioned consultative document published by the Basel Committee on Banking Supervision (hereinafter called the Basel Committee).

The German Banking Industry Committee (GBIC) welcomes the Basel Committee's initiative to incorporate lessons drawn from the financial crisis concerning an improved operation of the internal audit function and to revise the 2001 guidelines in this regard. In our view, when it comes to an effective verification of the appropriateness and effectiveness of risk management and of the internal control system, the internal audit function constitutes a crucial tool within banks. In order to ensure high quality work in this respect, it would be judicious to arrive at a harmonised understanding on an international level concerning the minimum requirements and expectations with regard to the functional mechanism of the internal audit on the part of supervisory authorities. The present consultative document mostly lives up to this goal. One further positive aspect we should like to highlight is that the principles presented in the consultative document are geared towards the industry's best practice approaches and that they are, in part, derived directly from international standards e.g. those promulgated by the Institute of Internal Auditors (IIA). However, we would like to point out that, along with the IIA standards, a host of other industry specific standards exist on the national level which, in terms of their quality and level of detail, would appear to be at least on a par with the IIA standard. Hence, in our understanding, the reference to the IIA merely serves the purpose of exemplifying this.

Complex, globally acting banks will obviously have to meet higher expectations than banks with a limited scope of action and a simple business model. We therefore explicitly welcome the fact that the proposals made under the present consultative document shall be equally subject to the principle of proportionality inherent in pillar 2 of the Basel Accord.

Under the proposals contained in No. 5 of the present consultative document, the Basel Committee correctly points out that different organisational structures exist in the various countries which means that a uniform use of the terms board of directors and senior management will be difficult. Traditionally, in Germany a two-tier board system exists with senior management (executive board) taking care of the executive tasks and the supervisory board or, moreover, board of directors acting as a non-executive oversight body [dualist corporate structure]. Under this two-tier board system, the bank's external representation – including but not limited to the dialogue with the supervisory authority - will be performed by senior management (i.e. the executive board in Germany). In Germany, based on the foregoing, the internal audit function constitutes an instrument for senior management. There is a direct reporting line from the internal audit function to senior management and the internal audit function has to inform the latter by means of reports. Senior management is also responsible for approving e.g. the audit plan or the internal audit charter. Senior management, in turn, has to provide the supervisory body with information and reports. Notwithstanding the foregoing, if and when he or she directly involves senior management in this, the chairperson of the supervisory body may also obtain information directly from the head of the internal audit function.

The German banking community is under the impression that the principles developed by the Basel Committee are strongly predicated on a system within which the internal audit function reports to the supervisory body and where the implicit assumption is that the supervisory body shall feature a close proximity to corporate executive processes or, moreover, the audit processes [monistic corporate

structure]. Yet, especially in Germany, more often than not, this does not tend to be the case. However, one prerequisite for an appropriate explanation of audit findings consists in, at least, technical proximity as far as the underlying subject matter is concerned. Hence, we would welcome it if the Basel Committee's forthcoming proposals were to take said corporate organisational systems into greater account.

Based on the foregoing general remarks, we would like to share the following, more specific comments on the principles and points raised in the consultative document.

## Specific comments

### A. Supervisory expectations relevant to the internal audit function

**No. 12**

We feel it would be appropriate to take account of existing organisational systems (cf. also our foregoing remarks); essentially, the principles ought to become more open in this respect. Hence, an approval of the audit plan by senior management should be equally permissible. One possible way of involving the audit committee in this process would be that it shall receive a report on the audit plan previously prepared by the internal audit function and adopted by senior management. Based on this, the audit committee or the board of directors may then decide on the need for potential additional amendments.

**No. 14**

The Basel Committee recommends that, whenever practicable and without jeopardising competence and expertise, the internal audit staff should rotate periodically within the internal audit function. In view of the growing complexity of the methods and processes deployed in bank control as well as risk management along with the corresponding need for specialist knowledge, we feel that such a proposal is unrealistic. In our opinion, rotation would rather lead to a deterioration of the audit findings' quality. This cannot be compared to a rotation of the external auditor because even if an external audit firm holds a mandate over a longer period of time, it will only be the head of the external audit team who will rotate after several years - there will be no replacement of the entire audit team.

**No. 15**

We agree with the Basel Committee on the need for avoiding conflicts of interests when it comes to the internal audit function. Hence, the Basel Committee proposes that the remuneration of the internal audit function's staff must not be linked to the financial performance of a business unit for which they exercise internal audit responsibilities or to that of an underlying business. We feel that a general prohibition of tying remuneration to a bank's business performance would be both inappropriate and practically unfeasible. Already on the grounds of equal opportunities and under the proviso that this does not result in any perverse incentives, also staff members working for the internal audit function should be entitled to benefit from a positive business performance. We therefore suggest deleting the last half of the sentence. Furthermore, such a deletion would be consistent with the provisions under the FSB Principles for Sound Compensation.

**No. 17**

The Basel Committee is of the opinion that the internal audit team, collectively, should be competent enough to examine all areas in which the bank operates. On a precautionary note, we would like to point out that an agreement on outsourcing of internal audit tasks to external parties is motivated by the very

need to hire specialist expertise due to the absence of on-site expertise in this matter which may be due to the sheer scope of the audit and the rare relevance of the subject matter at hand. At this juncture, the proposal sets out that an adequate transfer of knowledge from external experts to the bank's internal audit function needs to be ensured. In our understanding this should only signify that in the event of a follow-up or of a renewed audit as part of the regular rotation, the internal audit function shall, once more, be entitled to resort to external expertise. Otherwise, this proposal would repeal the bank's outsourcing right in a way that would be rather detrimental for the bank.

**No. 23**

Under the present proposals, the internal audit charter should be made available to all internal and external stakeholders and interested groups. Due to the absence of any further explanation we do not comprehend why the audit charter should be made accessible to stakeholders and other interested parties such as trade unions, financial authorities or other lobby groups. By definition, the rationale behind the internal audit function and its mandate are located inside a bank. This means that this internal function cannot deliver any value added to these external parties in terms of assessing the bank's risk management as well as its financial situation and its assets and liabilities. We therefore suggest deleting this proposal.

**No. 25**

Under the Basel Committee's current proposals the internal audit function shall be empowered to examine any activity or entity, and to access any records, files, data and physical properties of the bank. We should like to point out that the internal audit may only act within the bounds of existing legislation and has to take account of earlier requirements, e.g. data protection law or collective labour law.

**No. 27**

According to the proposals set out under No. 1 and No. 26, the internal audit function should primarily evaluate the effectiveness of the internal control framework. Pursuant to the proposals under No. 27, however, the internal audit function's remit shall also include an assessment of the operational workflows. The internal audit function's prime responsibility consists first and foremost in the identification of potential shortcomings in a bank's processes and procedures. Hence, the internal audit function should focus on a functioning and appropriate internal control framework. Efficiency, on the other hand, should only play a subordinate role.

**No. 29**

We feel that preparing an annual internal audit plan which is based on the results of a risk assessment is generally useful. However, from our point of view, it is important that audit intensity and audit scheduling be closely correlated to the underlying risk. Hence, we suggest the following amendment to the third sentence: "The head of internal audit should ensure that all entities and all activities of the bank are audited at least once within an appropriate period of time (audit cycle) <u>to a level of work commensurate with the assessed level of risk."</u>

We also propose more detailed explanations concerning the Basel Committee's expectations as regards "... input from... the board..." and in which shape and form such input ought to be provided.

**No. 30**

We agree with Principle 7 and its explanation under No. 30 pursuant to which the internal audit function shall ensure an adequate coverage of the regulatory matters within the audit plan. This requirement is

already inherent in the internal audit function's core mandate; hence, there is no need for a separate emphasis thereof.

**No. 40**

In our view, the communication channel between the banking supervisor and the internal audit function illustrated in Annex 1 is too far-reaching (cf. also our comments on the proposals under No. 71 and No. 72).

**No. 43**

According to the proposals under No. 43, the board of directors or the supervisory board should review the effectiveness and efficiency of the internal control framework at least once a year; if needs be, it should also consider commissioning an independent review of the internal audit function. However, at least in Germany, such independent reviews are already part and parcel of the external audit. We propose accepting the review performed by external auditors as equivalent to said independent review.

**Principle 10 in conjunction with No. 48 to No. 50.**

On principle, an approval of the audit plan by the audit committee would be incompatible with the corporate governance structure which has been tested and tried in Germany. Here, the entire senior management team (Gesamtvorstand) is responsible for approval of the audit plan. We can think of but few exceptions to this rule, for instance only in those cases where senior management representatives from the parent company will be on the subsidiary's audit committee.

In our view – depending on the organisational structure – also senior management should have the right to approve the audit plan. The corresponding information will be forwarded to either the audit committee or the supervisory body.

**No. 53**

Under the present proposal, the internal audit function shall be accountable to the supervisory board or, moreover, the board of directors and its audit committee on all matters related to the performance of its mandate as described in the internal audit charter. According to the higher-ranking Principle 12, the internal audit function should report to the audit committee or the board of directors or, moreover, the supervisory Board and at the same time it would have to inform senior management. However, in Germany, the internal audit function is an instrument of senior management. It is directly accountable to senior management and has to report to the latter. Hence, in terms of HR and the scope of its mandate, the structure and activity of the internal audit function shall always be determined by senior management (the Vorstand) of a bank. The supervisory body is therefore especially responsible for overseeing senior management's management function.

In our view, it is of crucial importance that the internal audit function reports to one party only. In a two-tier model like the one which exists in Germany this would be senior management (Vorstand). In a system such as the one which exists in Germany, the audit committee's responsibilities listed in Annex 2(b) to (o) for the internal audit would be met by the German-style executive board (Vorstand), or, moreover, a bank's senior management.

**No. 54**

We agree that senior management which is responsible for an adequate control framework should be informed by the internal audit function of all significant findings. At the same time we feel it is appropriate

to bring audit findings to the attention of the departments concerned, too. This way, shortcomings can be addressed in a timely manner.

Under the present proposal, the head of the internal audit function shall have to prepare reports to the supervisory body or to the audit committee concerning the status of those findings which have not yet been remedied by senior management. We feel that this reporting requirement is extremely far-reaching. We suggest an escalation procedure for this reporting requirement. In other words, the reporting requirement should only apply to overdue significant findings that have not been rectified on time.

Principle 13 in conjunction with No. 55 f.
Under the current proposal, the internal audit function is assigned a complementary role. In our opinion this implies that the internal audit function's remit as a process-independent part of risk management – i.e. the situation to date in Germany - is and will remain clearly separated from the operational, process-dependent activity.

This also applies to the proposal under No. 56 pursuant to which control failings by one line of defence should, in principle, be detected by another line of defence. In our opinion, this can be met primarily by a corresponding on-going mutual control of the individual functions. However, de facto, this provision might result in confusion of responsibilities as well as duplication of controls and hence uneconomical workflows in a bank. It should therefore be deleted.

**No. 58**
In our understanding, No. 58 gives a description of a compliance function under the Anglo-American model. Contrary to the securities compliance under the German rules and regulations, the this Anglo-American modelcompliance function described in the consultative document monitors the risks of non-compliance with statutory requirements in general. The remit of the compliance function described under No. 58 obviously also covers money laundering, anti-fraud and data protection. In Germany, there is an in-depth debate on such a business orientation of the compliance function with regard to its implementation in terms of setup and organisational matters . Hence, it is even more important that the Basel Committee provides a clear-cut idea of its understanding when it comes to the existing control functions such as risk management, compliance and internal audit function.

**Principle 14**
Basically, we support the principle pursuant to which the internal audit function shall be centrally shaped by the parent company in a group structure or in a holding company structure. In this context, however, in addition to the responsibility of the parent company's senior management, it will be necessary to explicitly also take into account the subsidiaries' oversight bodies competencies as defined by the respective company law and the respective prudential supervision. Especially the roles and responsibilities mentioned in this principle need to be geared towards the respective national existing provisions. For instance the organisation of the subsidiary's internal audit function can and must not be defined without the due and proper involvement of the subsidiary's competent bodies. There needs to be a basic clarification as to who exactly (i.e. someone within the parent company or someone within the subsidiary company) shall be in charge of said tasks.

**No. 62**
At this juncture, the Basel Committee proposes that every activity (including outsourced activities) and every entity of the group should fall within the overall scope of the internal audit function. In our understanding, one possible reading of this provision is that the parent company's internal audit function

shall have to audit each and any activity and process as well as units of the group companies within a specified time frame – regardless of any audits that may have been performed over the same period of time by the subsidiary's internal audit function. In our understanding, the group audit should complement the group companies' internal audit as part of risk management. During said exercise it shall also be entitled to take into account and incorporate audit findings from the group companies' internal audit.

**B. The relationship of the supervisory authority with the internal audit function**

**Principle 16**

We welcome the fact that the interaction between the internal audit function and the supervisory authority shall be enhanced in the framework of the regular annual discussions. In view of Germany's existing system pursuant to which the internal audit function shall be a control instrument of senior management, said communication between the supervisory authority and the internal audit function should not take place without the involvement of senior management.

**No. 71 and 72**

In line with its statutory mandate, the internal audit function acts on behalf of senior management. Its goal consists in ensuring the effectiveness and adequacy of the risk management systems as well as of the internal control system. Hence, the internal audit function should first and foremost report to senior management. In our view, the audit function's direct communication of its findings and measures to supervisory authorities would be problematic. We feel that senior management should be the prime interface for the supervisory authority and that, in such a capacity, it ought to coordinate information requests and reports. The same should apply to any oral communication between the supervisory authority and the internal audit function. In this context there would also be an opportunity for a regular exchange of information or, moreover, discussions on relevant matters between the supervisor and the internal audit function which can be constructive indeed.

**No. 73**

We welcome communication between the supervisory authority and the bank concerning the audit plan because it is generally useful. However, we are not sure whether the audit committee's chair would be the appropriate person to be contacted by the supervisors. In our view, the prime person to be contacted ought to be the head of the internal audit function.

We feel that a clarification would be in place, i.e. that only a significant divergence from the internal audit plan shall have to be discussed with the supervisory authority. During the regular meetings with the supervisory authority, the focus should rather be on significant, audit specific events. Furthermore, as far as the discussion of the audit plan for the forthcoming year is concerned, in our understanding this shall not hinge on an ex ante approval by the supervisory authority, or, moreover, there is no mandatory requirement to negotiate the draft internal audit plan with the supervisory authority.

**No. 75 to 80**

At this juncture, the proposal contains a list of potential topics for discussion between supervisors and the internal audit function. In our view, this list is too far-reaching. In order to meet its tasks, the internal audit function does not require the same level of data as operational controlling, accounting or group management nor does it have to analyse said data in a detailed manner on an on-going basis.

**Comments "The internal audit function in banks"**

In our understanding, it is furthermore not incumbent upon the internal audit function to evaluate (on an ongoing basis) specific results determined during the assessment of risks or, moreover, balance sheet items and performance ratios. We feel that this is the role of risk management or accounting. Rather, the internal audit function's remit consists in auditing processes and procedures in said areas in order to verify whether they are appropriate. Hence we would like to propose the following complementary amendment to No. 78: "To the extent that accounting data drives certain regulatory measures or is included in regulatory reporting, supervisors should seek to understand and benefit from work performed by internal audit on processes and controls relating to: […]".

Furthermore, many of the aspects addressed under No. 77 to 79 either concern the bank's senior management, the external auditor or the compliance function. In our view, these aspects should be covered by the respective functions.

**C. Supervisory Assessment of the internal audit function**

**Principle 17, No. 82 to 87**

According to the Basel Committee's current proposals, the supervisory authority should regularly assess whether the internal audit function has an appropriate standing within the bank and whether it operates according to sound principles. At this juncture, in order to perform its assessment of the internal audit function, the supervisory authority should develop a grading system. Furthermore, the audit committee or its equivalent and the internal audit should develop and maintain their own tools to assess the quality of the internal audit function.

In this context we should like to point out that, in Germany also due to supervisory requirements, a regular assessment of the internal audit function is performed by the external auditors as part of their annual audit. Therefore, we would appreciate it if the Basel Committee were to incorporate into its guidance said relevant audits performed by external auditors under their statutory national mandate. First, in our view, the development of own tools should be left to the discretion of the bank. Furthermore, this should be subject to the principle of proportionality.

**No. 87**

At this juncture, the Basel Committee expresses the view that the appointment and replacement of the head of the internal audit shall be relevant for the bank's supervisory assessment. Therefore, under the current proposals, the supervisory authority should be promptly informed of the fact itself as well as its circumstances. Similarly, the supervisory authority should be entitled to arrange meetings with the former head of internal audit.

In our opinion, the information requirement during the appointment of a new head of the internal audit function is too far-reaching. As far as we can see, it is not immediately obvious which consequent additional insights the bank may possibly gain for its supervisory assessment. Similarly, the Basel Committee should abandon its plans concerning contacts to the former heads of the internal audit function. As long as the head of the internal audit function remains a bank employee in another function, he is bound by the employee relationship. In terms of labour law, it is unlikely that he will be under the obligation to make comments which may have detrimental implications for him. However, once the former head of the internal audit function has left the bank, he will hardly be under a legal obligation to make himself available for meetings with the supervisory authority.

## Comments "The internal audit function in banks"

**No. 94**

The Basel Committee is contemplative of making public supervisory actions that are aimed at remedying certain deficiencies in the context of the internal audit function. We are of the view that the banking supervisor already has ample opportunities for influencing management and the supervisory body in order to address corresponding shortcomings. Furthermore, a public disclosure might provoke a violation of other legal provisions, for instance in the field of data protection or banking secrecy. Hence, we reject the notion of making public supervisory action in this context.