The voice of banking
& financial services

29 February 2012

baselcommittee@bis.org
c/o the Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland

Dear Sirs,

The internal audit function in banks – consultative report

The British Bankers' Association ("BBA") is the leading association for UK banking and financial services for the UK banking and financial services sector, speaking for over 230 banking members from 60 countries on the full range of the UK and international banking issues. All the major banking players in the UK are members of our association as are the large international EU banks, the US banks operating in the UK and financial entities from around the world. The integrated nature of banking means that our members are engaged in activities ranging widely across the financial spectrum encompassing services and products as diverse as primary and secondary securities trading, insurance, investment banking and wealth management, as well as deposit taking and other conventional forms of banking.

The BBA is pleased to respond to the consultation.

Key messages

We welcome the update of the 2001 guidance.

We agree with the encouragement to set up an audit committee, but point out that some banks may have a committee that oversees audit, risk and compliance. The recommendation should be with regard to the nature, scale and complexity of the firm, as sections 7 and 41, and principle 10 suggest.

The document does recognise that all areas are within the scope of an internal audit function's responsibilities (e.g. section 26). However, whilst noting section 59, perhaps there is not due reference to the importance of a risk based approach and the importance of focusing on key risks.

We have no comments on the principles, but note that there is not a principle expressing the importance of Internal Audit taking a forward looking stance to develop and improve its effectiveness. Whilst this could be considered to be implicit in the comments in the introduction, a more explicit statement to this effect would reinforce the Internal Auditor's responsibility to continue to develop, evolve and improve.

British Bankers' Association
Pinners Hall
105-108 Old Broad Street
London
EC2N 1EX

T +44 (0)20 7216 8800
F +44 (0)20 7216 8811
E info@bba.org.uk
www.bba.org.uk

The paper is silent on the Model Independent Review function, which is an increasingly important one in banks. We believe that it is worthwhile commenting on this. One would expect there to be a close working relationship between the Internal Audit function and the Model Independent Review function, but it is appropriate that the two are distinct functions within a firm. We are seeing an increasing number of regulators mixing the two and we believe that supervisors should keep the boundaries.

Conclusion

The overarching tenor of the report is weighted heavily towards regulatory expectations, which we're assuming was intentionally the Committee's focus; however, the paper seems to only mention in passing the “bread and butter” activity of an internal audit function, i.e. the focus on the control environment.

The annexe to our letter contains our formal response to the consultation, and further specific observations and questions arising from the proposals.

We hope that you will find our comment useful. Please contact me by way of e-mail (irving.henry@bba.org.uk) or telephone on (00 44) 20 7216 8862 should you require further information.

Yours faithfully,

Irving Henry
Director, Prudential Capital and Risk

Annex

Principles 1 - 2

The European Union's third Capital Requirements Directive (CRD III) enshrines the independence of the control functions, including Internal Audit, by requiring their remuneration to be from a separate pot and oversight to that of the lines of business that they keep an eye on.

Section 14

This recommends rotations "within the internal audit function". This might be extended to recommend rotation within the wider bank. Some banks aim to rotate staff between Internal Audit and the businesses and other functions of the bank whilst remaining cognisant of the issues of avoidance of conflict cited in section 21.

Sections 15 - 21

Section 15 indicates that the independence of Internal Audit may be undermined by remuneration linked to the performance of the areas audited. However, it gives no indication of regulatory expectations and further clarification here would be beneficial. In addition, the reference to compensation in section 21 might more logically sit under section 15 to provide a concise view of regulatory remuneration expectations in relation to Internal Audit.

Section 21 refers to a "cooling off" period during which internally recruited auditors should not engage in auditing activities in areas for which they had previous responsibility. Periodically, banks use short-term secondees ("guest auditors") from the business who can provide additional expertise and insight. The required separation could be achieved for "guest auditors" by ensuring that they would not be responsible for directly auditing the part of the business for which they were responsible. For example, a "guest auditor" might be brought in from one geographic region to assist with the audit of the same function in another geographic region. Or in the case of the audit of a head office function, a "guest auditor" from that function might be used to provide specialised knowledge of that function, but would not lead the audit. We would suggest that this be suitably clarified.

Sections 23-25

In practical terms, a charter contains the key elements of audit policy and it would be helpful if the guidelines recognised that a properly structured and approved policy framework is a suitable alternative to a charter.

Principle 6

UK law specifies that the outsourcing of activities does not absolve and/or limit the liability of the party that contracts out its activities. UK regulators expect such parties to monitor activities carried out on their behalf.

Sections 26 – 7

Section 26 highlights the importance of the examination of the effectiveness of the control environment. However, Section 27 uses the term "effectiveness and efficiency of the operations". Whilst welcoming the opportunity to comment on the efficiency of the operations if required, we feel that reviews of efficiency should be of lesser importance than effectiveness of the control environment. It should be at the discretion of the audit committee as to whether they are part of Internal Audit's mandate. We therefore recommend that "and efficiency" is deleted as it should not be a minimum requirement.

Section 27 states that Internal Audit should monitor compliance with laws and regulations. Whilst the requirement is understandable, in many organisations the Compliance function is primarily responsible for this task. Internal Audit should seek to discharge this responsibility, where appropriate, through reviewing the Compliance function including their monitoring capability and effectiveness and we would therefore suggest that this is linked to sections 37 - 9.

At present the requirement to “evaluate the effectiveness and efficiency of operations” is not a key focus for an internal audit function, most notably the comments around “efficiency”. Whilst an internal audit function will review the effectiveness of controls, the effectiveness and efficiency of operations is not the prime focus although bank auditors may bring any material issues to management's attention if they come across them as part of our normal activities.

Section 29

The document does not make clear whether the annual audit plan has to include a detailed audit plan for the full year. For the avoidance of doubt we would propose that whilst the audit plan will be reviewed and updated at least annually, the period for which specific audit plans are made may be less that one year. This is consistent with ongoing, real time assessment of where key risks lie. This is also relevant to section 73 which requires that any variances to the annual audit plan have to be explained to the relevant supervisor.

Further, this section goes on to state that, “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).” Reference is also made to section 26, which refers to “the effectiveness of the internal control framework of the entire bank”.

Noting our points in the opening paragraph we fully support the establishment of an annual plan based on a risk assessment. The level of audit work undertaken each year in any area should be proportionate to the risk. Accordingly, we would suggest that wording should stress the importance of a risk based audit framework which ensures the risks of the organisation are properly assessed and prioritised with audit coverage being scheduled on a flexible basis to provide timely assurance that risks are being managed. Accordingly, the third sentence of the section might be updated to read, “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) to a level of work commensurate with the assessed level of risk.”

Finally, the role of the Audit Committee should be to satisfy itself that the approach / methodology in place is appropriate for the organisation, properly implemented and that they are informed as necessary on plans and outcomes. The requirement of a "cycle" can be construed as contrary to the spirit of such an approach. As such, in fulfilling its responsibility to ensure that all areas are subject to appropriate coverage according to the risk profile Internal Audit may not touch at all upon some entities within any given cycle.

Principle 7 and sections 30 – 9

These sections provide greater direction in terms of what is required to be audited in relation to regulatory matters than appears elsewhere in the document for other areas of risk. Whilst perhaps understandable given the context for the proposed revisions of the 2001 document, and some shift of emphasis may be desirable, this may have the effect of overly skewing the focus of audit work onto regulatory areas rather than the broader range of risks (of which regulatory risk is a part) within the business.

Sections 32 - 4 are skewed towards the capital framework; perhaps there should be an equal focus on liquidity in light of the banking crisis.

Principle 8 and Section 41

This requires each bank to have its own permanent internal audit function. However, Principle 14 indicates that the internal audit function in a group structure or holding company structure would be established centrally by the parent bank and Section 60 indicates that the board of directors and senior management of the parent company have the overall responsibility for ensuring that an adequate and effective internal audit function is established across the group. The BBA is aware that some banking groups effectively operate their internal audit functions on a group basis rather than requiring each bank or organisation within the group to maintain its own internal audit function. Therefore, we would suggest that it should be made clear that the latter requirement takes precedence over the former and that it should not be a requirement for any and all separately incorporated entities to maintain its own audit function unless “the board of directors and senior management of the parent” deemed this necessary.

Principle 11

UK law requires that the appointment of the head of internal audit be approved by the regulatory authority and demonstrates such qualities.

Section 54

This refers to Internal Audit's responsibility to follow-up on implementation of its recommendations. It would be helpful if this paragraph made clear that the primary responsibility for monitoring and reporting on the implementation of Internal Audit recommendations lies with management rather than Internal Audit (subject to Internal Audit being in a position to highlight any discrepancies in the reported data).

Principle 13

The UK Financial Services Authority’s Systems and Controls (SYSC) rulebook requires such control functions.

Section 56

We agree that downstream lines of defence should be picking up failings in upstream lines, but not the other way round (e.g. the first and second lines would not be expected to pick up failings in Internal Audit (third line)). The text should clarify this ambiguity for the avoidance of doubt.

The section indicates that responsibility for internal control does not transfer from one line to another and we are fully supportive of the principle that first line should not be dependent on second line checking in ensuring appropriate control of risk, and so on for the second and third line. However, it may be appropriate for ‘superior’ lines to place reliance on the work of others e.g. Internal Audit may determine that it is appropriate to place some reliance on work done by the operational risk function or the credit review function in the second line of defence, and this principle should also be recognised.

Principle 15

UK law specifies that the outsourcing of activities does not absolve and/or limit the liability of the party that contracts out its activities. UK regulators expect such parties to monitor activities carried out on their behalf. Service level agreements (SLAs) between the banks and contractors specify that the contractors adhere to the banks’ standards.

Section 72

We agree that supervisors should meet periodically with internal audit to discuss findings and recommendations, and note that this is already happening at our members with many of their supervisors. However, discussions on the progress of remediation of findings raised by supervisors should primarily be with the business and/or risk and compliance functions.

Section 73

We support discussions with supervisors on the audit plan, but consider the most appropriate person to be contacted by supervisors to discuss these matters is the ultimate head of audit. If required, the matter should be escalated to the management board, and only as a last resort to the chair of the audit committee.

This requires supervisors to understand reasons for changes in audit plans. This may be an overly prescriptive requirement and should supervisors wish to understand reasons for changes in plans they would always be entitled so to do. A requirement might prove to be both time consuming and a distraction from more significant matters.

Section 74

This indicates that supervisory authorities may consider sharing relevant information with Internal Audit. A more directive approach, which would require sharing unless there was a pressing reason not to share, would be welcomed. The requirement in section 28 for Internal Audit to "develop an informed and independent view of the risks faced by the Bank" supports this approach.

Sections 75 – 8

Audit work on judgmental matters will necessarily focus on the effectiveness of the processes and controls used to arrive at the judgment, often tested by sample testing of particular judgements. It will not necessarily opine on specific balances.

We therefore suggest that the first sentence of section 78 is updated to read, “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:…”

Annex 1

This sets out all linkages for Internal Audit, but also includes some linkages for non-Internal Audit areas, e.g. external audit to the board whilst excluding linkages in other such areas, e.g. senior management to the board.