Response to Basel Committee's Consultative document "The internal audit function in banks"

1) All views in this document are represented only on behalf of the author.
   None of the opinions or views exposed should in any case be attributed to his present and past employers or professional bodies in which he is a member.
2) Given my limited interaction with supervisors, the comment relates to the 15 principles under the "Supervisory expectations relevant to the internal audit function".

General comment

As a professional with 11 years' experience within financial services audit (6 of them within internal audit), is my honour to have this opportunity to provide comments on the consultative proposal issued by the Basel Committee in December 2011.

Overall, I agree with your proposal. The 15 principles described under the first section are reasonable and describe many of the best practices I have seen within internal audit.

Observations

Despite the overall positive comment, I would like to bring to your attention to two observations.

Both try to highlight to the Committee that the internal audit function within the banking sector tends to be surrounded by a more developed risk framework than many of our internal audit colleagues in other sectors. Thus, the Committee could go a step further setting the principles to a higher standard.

A) Internal Audit "recommendations"

Analysis:
In five times in the proposal the Committee refers to the "internal audit findings and recommendations". In my career, I have seen the word "recommendation" applied sometimes to refer to an opinion (where the auditor proposes management to take a more or less active stance to improve the control environment) and sometimes to a mitigating action plan suggested by the auditor. The observation is given if the Committee took the second meaning.

Given that the goal of a bank is to embed the concept of three lines of defence referred in principle 13, the ideal scenario is one where the first line of defence is responsible to mitigate the risks to the bank: *"57. Operational management has ownership, responsibility and accountability for identifying, assessing, controlling, mitigating and reporting on risks encountered in the course of a bank's business activities".*

While I agree an internal auditor should help the first and second line to enhance the control environment where needed, I believe is worth to reinforce as much as possible that finding the resolution to a risk is responsibility of the first line, then the second line and, afterwards, the third line. Thus, my personal view is that the auditor primary role within a bank should be to identify weaknesses in the control environment to make all the lines aware of a particular risk.

Risk:
The risk an internal auditor faces when suggesting action plans is that the independent opinion may be impaired. A "recommendation" will more likely than not be a new control or a change in the control

design which contradicts principle 2 point 13. *The internal audit function should not be involved in designing, selecting, implementing or operating specific internal control measures*.

This point is best practice. If, at closure, the "new design" still leaves a significant residual risk to the firm, the internal auditor may decide to close the finding to avoid "losing face" despite his "recommendation" been unsuccessful in mitigating the risk.

Suggestion

- Clarify what the Committee understands by a "recommendation".
- If it refers to a suggested mitigating action plan. Clarify whether it is best practice that the mitigating action plan comes from the first line and second line as opposed to the third line given they are more familiar with the control environment and they are the owners of it.
- Additionally, the Committee may consider adding that if any of the three lines can't produce an acceptable cost effective mitigation plan, the finding should be risk accepted and monitored by management.

B) Audit role regarding Sarbanes-Oxley Act

Analysis:

I am sure the Committee is aware that US Sarbanes-Oxley Act Section 404 requires management and the external auditor to report on the adequacy of the company's internal control on financial reporting and Section 302 mandates the signing officers to certify that they are "responsible for establishing and maintaining internal controls" and "have designed such internal controls to ensure that material information relating to the company and its consolidated subsidiaries is made known to such officers by others within those entities".

In that respect, it does not differ too much from the fourth data element within an operational risk Advanced Measurement Approach, the Business Environment and Internal Control Factors.

During the initial implementation period, the certification work was taken on by some internal audit departments to reduce the overall cost the Act brought into their companies.
Later on, some of these internal audit departments transferred the certification process to the relevant line of business; this was specially the case after the US regulators clarified the extent of external auditors' reliance on management testing. However, some internal audit departments retained its former responsibilities.

In this case, the role of Internal Audit regarding Sarbanes-Oxley certification is unique; the third line neither owns the control environment nor has any decision power around coverage or sample testing, as is mainly driven by the external auditor.

This model omits that in the banking sector, as a difference to many other sectors where Sarbanes Oxley is also applied, there is a requirement for a more developed risk and control self-assessment which usually relies on formal first and second line of defence attestation processes.

The only rationale to support the existing model, given to me within a decade, was on the grounds of the Internal Audit skill set, which does not really make much sense as the internal auditor background tends to be very similar to those of people in charge of financial reporting.

Until today, I can't still see what makes Sarbanes Oxley different to any other management risk self-assessment process.

Risk:

- There is a loss of a line of defence on financial reporting as effectively the second line relies on the third line to carry the attestation.
- It sets the wrong incentives for the second line to improve and automatize its controls (as the cost of SOx compliance is attributed to the whole firm).
- Unfortunately, given its legal framework, the auditor can't use a risk-based approach (as per principle 2 point 14). This can create higher turn-over and thus, reduce the skill-set of the internal audit department (to minimise this impact, most internal audit departments outsource or co source SOx certification work).

Suggestion

- Determine whether it is best practice for the second line of defence to own the SOx control attestation as they do with any other standard risk control assessment or it is an accepted practice to have the third line doing the attestation on behalf of management.
- Consider whether management should oversee the impact of SOx coverage in an internal audit department in terms of extra budget, staff motivation, audit plan coverage impact, etc.