



## **AUDIT COMMITTEE CHAIR EVENT**

### **RISK ASSESSMENT AND MANAGEMENT**

Risk assessment and risk management are now near the top of every board's agenda.

When we met nearly one hundred company chairmen last year as part of our review of the UK Corporate Governance Code - including around sixty percent of the FTSE 100 - we started each meeting by asking them what their boards were doing differently as a result of what they observed happening in the banking sector. Almost without exception, the first answer was "spending more time thinking about risk".

And if any of them had been inclined to believe that risk was only a matter of understanding and managing financial risks, the example of BP has demonstrated very vividly that is not the case.

When we updated the Code earlier this year we added a new principle which states that boards are responsible for determining the nature and extent of the significant risks they are willing to take in achieving their strategic objectives.

Which begs the question - how do you do that in practice?

I won't pretend we have a ready answer.

That is why we decided to defer the update of the Turnbull Guidance that we had originally planned to start last month. We felt it was premature to attempt to define good practice before it had the chance to develop.



There is a lot of deep reflection going on in boardrooms and committees at the moment, and the FRC needs to tap into that.

So we intend to hold a series of meetings in the New Year to discuss this issue. We will be inviting a selection of board chairs, audit and risk committee chairs, executives, investors and advisers to share their views and experience with us. Only then will we decide how the FRC can most usefully help boards and committees to answer that question.

In order to answer the question of how to determine the nature and extent of the risks you are willing to take on, a lot of other questions have to be answered as well. For example:

- What are the respective roles of the board, board committees and management, and how do they interact? Where does oversight end and operational management begin?

The answer may differ from company to company, but there needs to be clarity about the remit and reporting lines. Otherwise there is a danger of confusion over who is ultimately responsible. The CEO clearly will have a key role in making sure the system works effectively.

Wherever the lines are drawn, the board has to demonstrate genuine leadership and commitment.

- What are the risks that the board needs to “own”?

The board needs to provide top down input to the risk assessment process and to supplement the understanding of the operational risks that comes from the bottom up. A well-constituted and effectively functioning board will be able to draw on the experience of the non-executive directors and identify emerging threats to the company’s future prospects.



- What information and advice do the board and audit committee need to carry out their responsibilities?

This seems to me to be one of the trickiest issues. The judgements boards and committees make can only be as good as the information on which they are based. How do you know whether you are getting that information? Is it being produced in a usable form, so you do not find yourselves looking for a needle in a haystack? And are the assumptions that have been made in preparing it made clear, so that they can be challenged if necessary?

Perhaps the board and committee need to spell out to the executives much more clearly what information they require. And perhaps they also need to consider how they satisfy themselves that there are internal assurance systems in place which would ensure that information is robust.

- How do they obtain confidence that the risk management and internal control system function effectively at operational level?

The board and audit committee should not be involved in micromanaging the risk management and internal control system, but either directly or indirectly they need to know enough to assure themselves they are working effectively. How do you strike the right balance?

- And how do they report effectively on these issues to shareholders – this is something that Bill Knight and Brendan Nelson will be discussing in the next session.

All of these are questions that will be on the agenda for the meetings we will be holding next year.



One thing we did not change in the Code was the provision stating that, in the absence of a board risk committee, either the audit committee or the whole board should be responsible for reviewing the risk management and internal control system.

During our review we raised the issue of whether to follow Sir David Walker's recommendation that banks should establish separate board risk committees, and recommend this practice for all listed companies.

Some commentators agreed with his argument that risk management was essentially a forward looking process, which did not fit well with the role of the audit committee, which they characterised as looking backwards, dealing with historical information.

But the majority argued against mandating risk committees for all listed companies. Some felt that in the absence of particularly complex risks, such as those present in the financial sector, there was no need for a separate risk committee. Others argued that, where there had been problems in other sectors, this often stemmed from the board having not spent sufficient time assessing the risks – a weakness that would not be remedied by creating another committee.

In the end, we concurred with the majority, and felt that the decision on whether to have a separate risk committee should be left to individual companies.

Where there is a risk committee, attention obviously needs to be paid to the relationship with the audit committee. There is a danger of overlap or – of greater concern – of issues getting missed entirely as each considers it to be the other's responsibility.



Various ways of managing this problem have been suggested, for example, common membership, common secretariat, joint meetings. But again that is an issue that needs further consideration.

I have shared with you some of the questions as we see them. There will probably be others I have overlooked. Nobody disputes the importance of risk assessment and management, but equally I doubt anybody would claim to have cracked all aspects. At the FRC we are keen to learn from your experience, and if my remarks have sparked any thoughts I would encourage to contact us to share them.

**Stephen Haddrill**

6 December 2010