Financial Reporting Council

Boards and Risk

A summary of discussions with companies, investors and advisers

September 2011

Introduction

The UK Corporate Governance Code issued in May 2010 states that "the Board is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives… [and] should maintain sound risk management and internal control systems".

Earlier this year the Financial Reporting Council held a series of meetings to learn more about how boards were approaching these responsibilities in rapidly changing markets. Participants from over 40 major listed companies - including chairmen, executive and non-executive directors and heads of risk and internal audit – discussed the issues involved in assessing and managing risk, as well as the difficult question of how such decision-making and risk management could be reported. Also involved in these discussions were a selection of investors and advisers. In addition, a number of organisations closely involved in this work kindly arranged for us to meet some of their members to get their perspective.

The FRC drew three main conclusions from these discussions.

The first was that there has been a step change in the Board's focus on risk in the last few years, at least in the companies that we spoke to. This conforms to the emphasis in the revised Code on the Board's responsibility for strategic risk decision-making.

The second was that while 'Internal Control: Revised Guidance for Directors' ("the Turnbull Guidance") was still broadly fit for purpose, some change was needed to reflect the role of the Board as articulated in the new version of the Code. The FRC intends to carry out a limited review during 2012.

The third conclusion was that the approaches and techniques used by boards have been developing rapidly. One size very definitely does not fit all, but there were some common themes and techniques found to be useful. We therefore felt that the insights gained about the issues boards were facing, and the ways they were addressing them, should be shared more widely to reflect and contribute to best practice.

That is the purpose of this report. It is not an attempt to provide guidance, and should not be seen as such. Rather it is an attempt to capture contributions from companies, investors and advisers in the belief that these may be helpful to other companies in thinking about their own approaches to risk.

The FRC would like to thank, most warmly, all those who participated in the various meetings for their time and insights. If readers find this report of interest, it is entirely due to the quality of the discussions it records.

Baroness Hogg
Chairman, Financial Reporting Council
August 2011

Summary of the Main Findings

1. The Board's overall responsibilities included determining the company's approach to risk, setting its culture, risk identification, oversight of risk management, and crisis management.

2. However, better risk decision-taking should not automatically mean less risk-taking, which was essential to entrepreneurial activity.

3. Different board committee structures may be appropriate to different industries and companies. The decision should be left to individual boards, rather than impose a "risk committee" on all companies.

4. While views differed on the exact dividing line between the Audit Committee and the Board, and between the Audit and Risk Committees, the essential requirement was clarity. Responsibility for reviewing internal controls and the process of risk management might be delegated to board committees, but this did not detract from the Board's strategic responsibility for risk decision-taking.

5. The Board needed to agree its appetite or tolerance for key individual risks; to understand the company's exposure to risk and how this might change, as a result of changes to strategy and the operating environment; and to take a view on these changes.

6. Boards needed to focus especially on those risks capable of undermining the strategy or long-term viability of the company or damaging its reputation.

7. Reputational risk had grown in importance and required greater attention. The increased "velocity" of risk, with near-instantaneous global transmission of failure, required robust crisis management plans, including clear prior agreement on the respective roles of the Chairman and Chief Executive in a crisis.

8. Boards are striving to develop new approaches for risk discussions and decisions, and to ensure that "risk maps" are actively managed and reviewed and focus on areas of change.

9. A focus only on "net risk" could be dangerous. It was essential that boards had a view on the company's potential exposure to risk. Boards needed a view of the combination of risks before the application of mitigation policies ("gross risk"), in order to consider their effectiveness.

10. One of the greatest challenges faced by companies was judging how much information was required by the Board to perform its role, including determining when a particular risk should be brought to the Board's attention. The Chairman played a key role here, but senior executives carried responsibility to see that risks were properly reported to the Board.

11. Transparency and clear lines of accountability through the organisation were essential for effective risk management.

12. Within the company, risk management and internal audit functions continued to play a vital role. Their reporting lines to board committees must be clear.

13. The issue of whether external assurance or advice was needed and, if so, who was best qualified to provide it, depended on the nature of the risk and the company's own internal capacity and expertise. For example, where the Board had established a separate Risk Committee, it was generally felt that it was beneficial for any advice that was needed to be sought from a source other than the company's external auditors.

14. Good corporate culture was widely seen as essential to good risk management, and in this respect the Board needed to set the tone at the top. Boards were becoming more proactive in seeking to assure themselves about the risk and control culture in the company.

15. Investors sought more meaningful reporting on risk, for example through an integrated discussion of the company's business model, strategy, key risks and mitigation.

16. While commercial sensitivities were acknowledged as an inhibition on open reporting, it was helpful if companies could indicate to shareholders when and to what extent they believed their exposure to risk was changing.

17. The Turnbull Guidance was generally considered still to be an effective framework for the review of risk management and internal control systems. However, the majority of participants believed that it needed to be updated to address the Board's responsibilities as defined under the revised UK Corporate Governance Code.

The Role of the Board, Committees and Management

The role of the Board

Participants identified a number of different elements to the Board's responsibilities for risk. They were:

- determining the company's approach to risk;
- setting and instilling the right culture throughout the organisation;
- identifying the risks inherent in the company's business model and strategy, including risks from external factors;
- monitoring the company's exposure to risk and the key risks that could undermine its strategy, reputation or long-term viability;
- overseeing the effectiveness of management's mitigation processes and controls; and
- ensuring the company has effective crisis management systems.

There was greater awareness and discussion of risk at board level than had been the case a few years ago. This was primarily as a result of the credit crisis and high profile cases such as the Gulf of Mexico, as well as learning from things that had gone wrong for competitors, which many participants felt had led boards to recognise more fully the potential benefits of effective risk management. Risk was no longer seen as primarily a matter for management and board committees, as had been the case in some companies, and boards were now active rather than reactive in addressing the subject.

However there was less agreement about the extent to which this greater awareness and time commitment had led to improvements in practice. Some participants felt that risk assessment and management techniques and systems were becoming more sophisticated and more widely adopted; others doubted whether these improvements were widespread and reported a great disparity of practices between companies.

It was emphasised that greater awareness of risk did not necessarily mean that boards were less willing to take risks. Rather, it meant that they ought to have a better understanding of the nature and extent of the risks involved in pursuing their strategy, meaning that risks were taken on consciously not unconsciously and were monitored more effectively as a consequence.

The role of board committees

Board committees were used to ensure that the Board received good quality advice and information and to enhance the quality of oversight, not as a substitute for board discussion or decision-making. The committee structure through which this support was provided varied between companies. It was considered that ensuring there was an effective relationship between different board committees, and between the committees and the Board, was probably more important than the exact committee structure.

Most participants considered that it would not be appropriate to impose a requirement for board risk committees outside the financial sector. They were now commonplace in that sector, and have been adopted by some companies in other sectors. In addition, a number of the larger companies represented at the meetings had separate board committees responsible for monitoring some of the key non-financial risks facing the company (although these were not called risk committees).

While many felt that the complexity of the business and nature of the company's product should be the determining factors in selecting a committee structure, separate committees were more common among companies in sectors where they were exposed to significant safety, environmental or regulatory risks, such as pharmaceuticals and the extractive industries. Examples included compliance committees dealing with risks associated with product regulation and corporate responsibility committees dealing with ethical, environmental and safety issues.

The main argument put forward by those participants who favoured separate committees to address key risks was that audit committees were already heavily loaded and did not have the time to address risk properly, and that a different set of skills may be needed. On the other hand, opponents were concerned that an additional committee might create confusion about responsibilities and/or lead to risk being compartmentalised, particularly if the Board was tempted to delegate its own responsibilities to the committee.

Supporters of both positions gave examples of how the perceived shortcomings could be overcome. Where there were separate committees, this could be done, for example, by ensuring some common membership or by holding joint meetings at least once a year. Where there was a single committee, some companies split meetings into two halves – one for audit matters and the other for risk – and/or invited other board members to participate in meetings of the Audit Committee at which risk was discussed.

Participants from smaller companies pointed out that these issues were less important for them as all non-executive directors tended to sit on all board committees.

The role of the Remuneration Committee in linking risk management with remuneration was also noted. More attention was being paid to this linkage, after a period in which remuneration schemes had been criticised for creating incentives to ignore or even increase risk in pursuit of short-term goals.

The role of management

It was agreed that the role of management was to implement board policies on risk and control using effective processes and procedures. Management needed to understand the business and its risks and ensure that there was trust, openness and transparency between themselves and the Board.

There was also general agreement that the ownership and day-to-day oversight and management of individual risks were rightly the responsibility of executive and line management, rather than the Board, although the Board needed to assure itself that these responsibilities were being carried out effectively. This could be done, for example, by ensuring that responsibility and accountability for managing specific risks was clearly allocated to individuals at all levels of the organisation, and through direct contact between board members and those responsible for key risks.

Management was also responsible for identifying emerging operational risks and bringing them to the attention of the Board where appropriate, and for ensuring the quality of the information that went to the Board. Companies used different structures to ensure this was done effectively. Some companies, for example, had established executive committees to scrutinise the detailed risk reports from around the organisation, and to ensure consistency in, and a common understanding of, the information provided to the Board and board committees.

It was important that there was clarity within the company about the responsibilities of senior executives with respect to risk management. While financial companies typically had a designated Chief Risk Officer, this was not always the case in other companies. In some companies the role of Chief Risk Officer was attached to the role of Chief Operating Officer or Chief Finance Officer. While many participants felt that ultimate executive responsibility for risk should rest with the Chief Executive, there was variation in practice.

The Company's Approach to Risk

There were differing views about whether it was either necessary or possible for the Board to apply a single, aggregate risk appetite for the company as a whole, as opposed to having a clear view on its appetite or tolerance for individual risks. Many participants felt this was difficult, not least because of the difficulty of quantifying many of these risks and the company's limited ability to mitigate a number of them, including external risks. A view was expressed that it was even more difficult for non-financial companies than for financial companies, particularly companies or groups operating across different sectors and markets, given the diverse nature of the risks they were dealing with. It was also noted that risk appetite can vary over time.

Some participants felt that all that could realistically be expected of the board was to have a clear understanding of the company's overall exposure to risk, and how this might change as a result of changes in the strategy and operating environment. When developing the strategy, however, it was important for boards to agree their appetite or tolerance for individual key risks. At its simplest, it was suggested this could be done by articulating what types of risk were acceptable and what were not.

The Changing Nature of Risk

Most participants agreed that there was a distinction between operational and strategic risks. Some participants also identified other categories, for example project risks and catastrophic risks (external factors which were entirely outside the company's control). Participants also identified a broad range of risks associated with technological developments, from threats to business models (for example, for some media companies) to operational risks (for example, cybercrime, which had clearly increased in recent years and included a range of threats from petty fraud to competitor theft of intellectual property and commercial information).

Many participants felt that the role of the Board in identifying risks differed for different categories of risk, with the Board having particular responsibility for identifying risks linked to the strategy, or resulting from external developments such as geopolitical and regulatory change. These were characterised as "top down" risks, and contrasted to "bottom up" operational risks which it was the responsibility of management to identify and, where appropriate, bring to the attention of the Board.

These distinctions did not hold when it came to the Board's responsibility for managing risk. Many participants noted that some operational risks were just as capable of damaging the long-term viability or reputation of the company as strategic risks, and said that in its oversight and monitoring capacity the Board needed to focus of those risks capable of causing most damage to the company if they materialised, regardless of how they were classified. While the greater awareness of "Black Swan" risks was welcomed, this ought not to be at the expense of addressing more "traditional" risks.

There was evidence that boards were spending more time than previously considering key risks, both at board meetings and outside (for example, at strategy away days). It was important that it was a proper discussion not a form-filling exercise. The value came from the discussion, which could help the Board identify priorities and better appreciate potential outcomes.

The form these discussions took varied. For example, some would start with a blank sheet of paper, while others involved presentations from management or others, including external experts. Some companies asked board members and senior management what worried them most and why. Others looked back over the previous twelve months to identify what had caught them unawares or why they had missed their targets. In at least one company the Board received regular briefings on societal, political and other external developments so that they could consider the potential impact on the business. Another technique was to seek to identify the "embedded assumptions" in the business model and to test these against the changing climate in which the company operated.

Many participants from companies reported that, whereas previously each risk had tended to be looked at in isolation, there was increasing awareness that risks were sometimes interconnected and sequential, and of the cumulative impact and disruptive effect of a number of significant risks materialising at the same time. There was some evidence that techniques such as reverse stress testing were beginning to be adopted outside the financial sector, at least amongst those companies that participated in the meetings. Participants felt it was important for boards to challenge received wisdom and ask themselves what would be the worst thing that could happen.

In general, reputational risk was not considered a separate category, but a consequence of failure to manage other risks successfully. However it had grown in importance, not least because the "velocity" of risk had greatly increased. It was considered that the "grace period" that a company had to deal with a problem before it became reputationally, and consequently financially, damaging had been greatly reduced. News of failures or problems often now had an almost instantaneous impact. Reasons given for this included developments in media and communications, including social networking, and a general mistrust of large corporations.

For these reasons, and given the inherently unpredictable nature of many risks, many participants emphasised the importance of ensuring that flexible crisis management and disaster recovery systems and business continuity plans were in place alongside control systems. In crisis situations, the Chairman and Chief Executive had crucial roles to play, which needed to be defined and agreed in advance. Getting the internal and external communication right was as important as dealing with the source of the problem.

For some companies there were significant risks inherent in the supply chain and outsourced activities, which the company had little direct ability to manage but which could damage its reputation if they materialised. It was felt that in these instances the Board needed to seek assurance that the supplier or contractor shared the company's risk and control culture. One participant gave an example of their company refusing to work with some contractors because of concerns about those contractors' risk culture. This had reaped benefits as customers saw it as a sign that the company took risk and control seriously.

The Quality and Use of Information

Boards are striving to develop new approaches for risk discussions and decisions. The classic "risk map", identifying risks on scales of probability and impact, is widely used. It was generally agreed that directional indications on risks mapped in this way are needed for a meaningful discussion, and that it was important that boards ensured that "risk maps" were actively managed and reviewed and focused on areas of change.

Managing the flow of information to the Board was considered one of the most difficult challenges by many participants. If the information was too detailed it would not help the Board focus on the key issues. If it was too high-level the Board may not understand the assumptions that had been made about the extent of the risk or the effectiveness of mitigation, and it may provide them with false assurance. There was also a danger that too much reliance might be placed on models and "traffic light" systems that themselves made a number of assumptions that may be incorrect. The same issues arose in relation of information presented to board committees. It was important for the Board and committees to indicate to management what information they needed to do their job effectively.

It was widely agreed that a focus only on "net risk" after mitigation could be dangerous. Such an approach tended to obscure the true extent of the company's potential exposure and the interconnected nature of the risks being taken by the company. It was important that boards had a view of the risks before the application of risk mitigation policies ("gross risk"), in order to understand and challenge assumptions about the effectiveness of those policies.

Where boards had set their risk appetite or tolerance for individual risks, some companies also compared the net and gross risks to the "target risk", so that the Board could judge how close the company's current exposure was to that which it considered acceptable.

In discussing the increased velocity of risk and the ability of operational risks to damage the company if left unchecked, many participants raised the difficulty of judging when the Board should be alerted to a particular risk, while avoiding a situation where absolutely everything was reported to the Board. It was considered that there was a need for clear triggers to determine when risks should be brought to the attention of the Board, and that the Chairman and other board members needed to be involved in deciding the level at which these triggers were set.

Some companies had attempted to address this issue by drawing up lists of emerging risks that were presented to the Board alongside the more conventional risk registers. Emphasis was also placed on the importance of strong internal and external communications and the need for trust, openness and transparency at all levels of the organisation.

Sources of Assurance

It was agreed that effective risk oversight required clear line of sight and accountability through the organisation. There was no "right" approach but clarity was essential.

There were a number of sources of assurance on which the Board could draw. These included the board committees, although as some participants noted these committees in turn relied on assurance from elsewhere in the company. Many boards and committees now held regular meetings with managers from across the company to discuss the risks for which they were responsible and how they were being managed. The frequency and nature of these meetings varied, but the direct contact and accountability was felt to be important by board and committee members.

As part of their management assurance process, some companies had introduced requirements for managers to self-certify as to the effectiveness of the controls related to the risks for which they were responsible. Others were sceptical about the value of self-certification, as opposed to independent assurance provided by the internal audit or risk management function.

The risk management and internal audit functions continued to play an important role. They did so by providing objective, independent assurance to the Board and committees and by challenging and/or providing advice to line management. There were different views on the precise scope of the two functions and how they overlapped, with different models being adopted. It was important that there was clarity about the respective responsibilities and in the reporting lines. Many participants felt that it was important that these functions reported directly to the Board or board committees in order to ensure their objectivity and independence was not compromised.

Some of the companies participating in the meetings had developed "assurance maps" which identified the different sources of assurance around key risks and controls. Those who used such maps felt they helped focus discussion at the Board and in board committees, and to identify gaps which may need to be filled by internal or external sources of assurance.

The issue of whether external advice or assurance was needed and, if so, who was best qualified to provide it, largely depended on the nature of the risks and the company's own internal capacity and expertise. External audit firms were one potential source of assurance and advice, but would not always be the most appropriate one.

For example, where the Board had established a separate Risk Committee, it was generally felt that it was beneficial for any advice that was needed to be sought from a source other than the company's external auditors. On the other hand, it was felt that, particularly for smaller companies, the external auditor could sometimes be a useful source of general advice, for example by alerting boards to issues of which they were aware from their audit work with other companies.

Risk and Control Culture

Many participants highlighted the importance of embedding the right culture throughout the company, alongside any improvements in techniques and processes. There was particular emphasis on the need for openness throughout the organisation. This would enable management and staff to escalate concerns in a timely manner without fear. Good culture resulted in better judgement, which reduced the reliance on process and provided comfort to the Board and senior management.

It was essential that boards led by example and set the tone at the top in order to influence the behaviour of management and staff. This required leadership in particular from the Chairman and Chief Executive, who needed to be seen to live the values they espoused. This had been attempted in different ways, for example by the use of values statements and codes of conduct and by being clear about any risks or practices for which there was zero tolerance. Everyone in the organisation needed to understand the boundaries within which they could operate and the actions they personally had to take.

It was recognised that risk and control culture was one of the issues on which it was most difficult for boards to get assurance, although boards appeared to be making more efforts to do so, including through some of the approaches described in the previous section.

The risk management and internal audit functions could play an important role, as could reports from and discussions with senior management, but some directors felt that there was no substitute for going on to the "shop floor" and seeing for themselves. It was otherwise very difficult to judge whether risk awareness was truly embedded or whether it was seen as a compliance exercise. This in turn assumed that non-executive directors had a sufficient understanding of the business, which some participants noted may not always be the case.

The importance of ensuring that incentives were aligned with the company's strategy and risk appetite or tolerance in order to promote an appropriate culture was widely recognised. There were different views on the extent to which companies had succeeded in achieving this alignment.

One common approach was to ensure that responsibility for managing specific risks was clearly allocated to individuals at all levels of the organisation, and their performance was measured and reflected in how they were rewarded.

In some companies the Remuneration Committee had been given responsibility for considering how to align the company's approach to risk and control with its remuneration and incentives. Examples were also given of the head of the risk management or internal audit function submitting reports to that committee, for example on how the company was performing against certain key risks, or being invited to comment on the details of proposed incentive schemes.

Public Reporting

The majority of investors who participated in the meetings felt that there was scope for considerable improvement in reporting on risk and internal control. Most participants from companies acknowledged shortcomings in reporting, but many of them felt there were obstacles to more meaningful disclosure.

Some institutional investors said that they placed more importance on the assurance they received from discussions with boards and management than on the words in the annual report. This was particularly the case when it came to assessing the quality of risk management and internal control, for which their main source of assurance was the quality of the Board. That said, reporting could be improved and none of the investors found the current tendency to produce long lists of risks useful.

Investors felt that boards should focus especially on strategically significant risks, and that this might be done by linking risk reporting to discussion of the business model. Discussing changes to the strategy and how the company might develop in the future, and explaining the implications for the company's exposure to risk, might enable companies to air some key risks in a way that did not raise commercial sensitivities.

Participants from companies said that in their experience most investors rarely asked questions about risk or internal control. There was a general wariness about disclosing commercially sensitive information or information that, if disclosed, might bring about the very risks the company was seeking to avoid. Reporting on the company's risk appetite was felt to be difficult as risk appetite was not constant but varied over time and depending on market conditions, if it could be defined at all. The same could be said about the company's overall exposure to risk. However, some directors and risk managers accepted there was a need to find ways of conveying more useful information.

Suggestions for improving reporting included:

- integrating commentary on risk throughout the report, rather than treating it as a stand-alone section;
- specifically, linking reporting on risk to discussion of strategy and the business model;
- explaining changes in the company's risk exposure over the previous twelve months, as a result of changes to the strategy or business environment, and indicating if it might change in the future; and
- disclosing how key risks were being mitigated.

The proposals on audit committee reporting in the FRC's 'Effective Company Stewardship' discussion paper were also discussed. Some participants were concerned that the proposals might increase the length of the report without a corresponding increase in value. However other participants thought that audit committee reports that dealt with the main issues discussed by the committee, rather than simply describing process, would provide greater reassurance that the Audit Committee was operating effectively and properly discharging its responsibilities.

While a few companies stated that they were getting some or all narrative sections of the annual report assured before publication, there was little enthusiasm for external auditors to be given mandatory responsibilities for validating risk reporting. The reasons given included that it was not appropriate for the company's willingness to take on risk to be assured, as this was a strategic and commercial decision; and that except in relation to financial controls, it was felt that the audit firms did not necessarily have the expertise to assess risk management and internal controls.

The Turnbull Guidance

There was discussion of the relevance and usefulness of 'Internal Control: Revised Guidance for Directors' ("the Turnbull Guidance"), and whether there was a need for it to be updated.

Most participants felt that the guidance was useful, and had met its original brief by providing boards with an effective framework for overseeing risk management and internal control systems. There were differing views about the extent to which it helped boards with other aspects of their responsibilities under the revised UK Corporate Governance Code, such as considering the nature and extent of the significant risks they were willing to take. Views also differed on whether, and to what extent, any changes may be required, although it was generally agreed that – if the guidance were to be updated – it should avoid greater prescription.

Arguments given against updating the guidance were that it continued to be largely fit for purpose and that it was not possible to provide meaningful guidance on some aspects of the Board's role, for example assessing risk appetite.

However, the majority of participants favoured reviewing at least parts of the guidance. Arguments for a review included that it was necessary in order to affirm whether the guidance was still applicable, particularly given the changes in the environment in which companies were operating; that the guidance did not adequately reflect the link between strategy and risk that has been established in the revised Code; that the guidance did not adequately address cultural and behavioural issues; and that it would be helpful to refresh the appendix to the guidance, which identified questions boards might ask themselves and management.

Financial Reporting Council
5th Floor
Aldwych House
71-91 Aldwych
London WC2B 4HN
Tel: +44 (0)20 7492 2300
Fax: +44 (0)20 7492 2301
Website: www.frc.org.uk