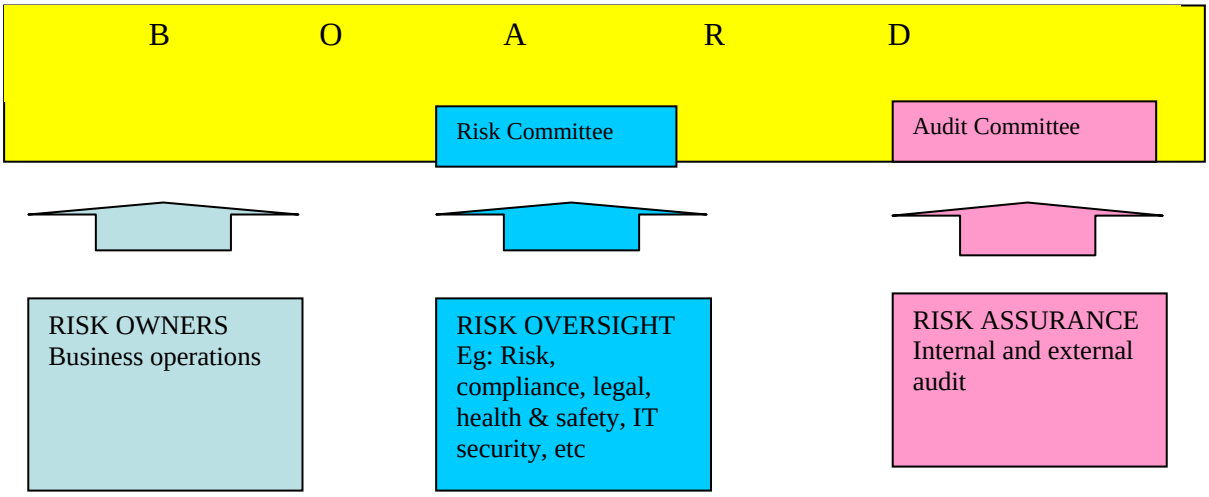
Governing risk: Untune that string and hark what discord follows

In January 2011, the Financial Crisis Inquiry Commission in the United States published its report on the causes of the financial crisis. It naturally picks out the contributions of poor mortgage lending standards, over-the-counter derivatives and the rating agencies. But its key conclusions about why the crisis was avoidable are that there were 'dramatic failures of corporate governance and risk management at many systemically important financial institutions' and that there was a 'systemic breakdown of accountability and ethics'.

These conclusions highlight the fact that risk management is primarily about effective frameworks of governance and about managing people risks. In this article, I shall deal with risk governance. Next month, I shall look at ways of managing the people side of risk.

The 3 lines of defence

Essentially, good risk governance relies on operating the three lines of defence, which are shown graphically below:



[Source: *Mastering operational risk*, Financial Times Prentice Hall (2010)]

The important thing is that each element of these groups points to the board, the second and third lines pointing specifically to the board risk and audit committees. The other point about the three lines of defence is that everybody in the firm understands precisely what their roles and responsibilities are in relation to risk management. And each knows what everybody else is meant to be doing. If it works properly, the firm will be like a well-practised orchestra. If not, all is discord and risk will be uncontrolled.

The board is where risk management comes together. Risk management is a core competence and responsibility of all directors. Risk should be fully considered in all major decisions. However, before that can happen, boards must articulate their

strategy and objectives and make sure those are communicated clearly throughout the firm. Too often the process is put on the 'too difficult' pile, other than a general statement about return on capital or something equally nebulous. If it's put on the 'too difficult' pile, then managing the business becomes too difficult. Strategy and objectives form the context in which to develop risk culture and risk appetites. Both of them reflect the balance of risk and reward of the board's corporate strategy. Or the board sets out its strategy and objectives, but then fails to tell anybody. Unless everybody knows what they are, effective risk management cannot happen.

The board sets the risk culture, not only in its statements but in its behaviour. The best way to see if that is effective is to see whether it's evident lower down the organisation. Professor Mervyn King, who chairs the King Committee reports on corporate governance in South Africa, memorably told the Institute of Internal Auditors' conference in September 2008, 'It's alright to talk about the tone at the top, but I prefer to think about the tune in the middle.' It's in the middle of the firm where you find out whether the culture articulated by the board is actually embedded.

So effective risk management starts with the board and the firm's strategy and objectives. Its risk culture will be determined by the board through the behaviour of individual directors. The culture and objectives will also influence the business decisions made by the risk owners, or risk-takers, in the business, the first line of defence. Which brings us to the second line, risk oversight and the role of the Chief Risk Officer (CRO).

The risk management function and the CRO

I will touch on two issues concerning the CRO: status and independence. In too many banks, the risk function fell from the top table and in some cases was not even at the table below that. The CRO became the Chief Reporting Officer, rather than somebody with authority and influence, a core member of the decision-making process and management team.

The CRO is not responsible for all risks in the business, a convenient scapegoat when things go wrong. Nor is it the CRO's sole responsibility to get risk management taken seriously. Both responsibilities fall to the board and risk owners. The CRO's key role is to ensure that the risk framework is effective and to provide challenge and oversight.

Should the risk management function, therefore, be independent? Where it holds a control or sanctioning authority and so provides the check and balance to the front-line sales function, it must, by definition, be independent. However, if it is overly protective of its independence, it can easily become divorced from the business which it is trying to analyse. When it comes to operational risk - the risks arising from internal processes and systems or from employees or from managing the impact of external events - the risk manager should be integrated into the business as an expert adviser and not become a remote and independent policeman.

One final point about risk and independence - the board's risk sub-committee. Following the Walker report and subsequent guidance from the regulators, there seems to be a view that the risk committee should involve only independent non-

executive directors. Given that risk is clearly the responsibility of all directors, whether executive or non-executive, I'm not sure that the Risk Committee should inevitably be made up of non-executives. Better that it's made up of those directors who can best make a contribution and provide appropriate oversight and challenge.

Independent assurance

The one truly independent function is that of assurance, or audit. The problem with internal auditors is that auditing processes, their principal role, can seem rather unsexy and so auditors move into risk management. Once auditors become part of the decision-making process, they cannot do their job. You cannot audit what you have agreed. If by any chance internal audit does act as a consultant for a particular project, it should be on the basis of a short-term contract, which is closely managed as such.

Audit should be independent, which also means that ideally its reporting line has to be to the Chair of the Audit Committee. Failing that, to the independent non-executive Chairman of the firm itself. Reporting to the CFO or COO is a fudge, despite protestations about being able to whistle-blow when required. Pay and rations is one thing; functional reporting is another.

Nor should it be the company's internal investigator. The risk function should be capable of and trusted in doing investigations. Audit can then validate its conclusions. If audit does perform an investigation, it should be at the direction of the Chair of the Audit Committee and nobody else.

Conclusion

Effective risk management starts and ends with the board. The board sets the tone of the risk culture of the firm. Both the culture and the firm's risk appetites (of which there will be many) will reflect clearly defined corporate strategy and objectives. But there is one final important component of risk governance, which is communication. If there are not open lines of communication both from the board down and, more importantly, from the lowest levels of the firm right up to the board, then the system will fail. The financial crisis was littered with examples of CEO's who were protected from bad news, or who ignored it when they were told.

In the first paragraph of its conclusions, the Financial Inquiry Commission paraphrases Shakespeare, 'the fault lies not in the stars, but in us'. Managing 'us' is the most critical element of risk management and the subject of my next article.

John Thirlwell is an independent adviser on risk management to boards in financial services and co-author of *Mastering operational risk* (Financial Times Prentice Hall, 2010).