Joined-up thinking

Risk management is an issue that has been highlighted in recent months – but how do you go about embedding it into your business effectively? **Julia Casson** and **Tony Hoskins** explain.

The governance, by the board, of a company's risk management process has been given enhanced focus following the introduction of a new principle into the proposed UK Corporate Governance Code.

This is a consequence of the view of many commentators that the poor management of risk, especially by boards, was one of the major contributory factors to the recent economic crisis. Whilst the causes of the crisis are complex and can be debated at length, events of the last year or so have certainly highlighted inadequacies of risk management. Boards have been criticised for not taking the risk process sufficiently seriously and failing to ensure board members' perspective is properly established on both risk tolerance and appetite – and managed accordingly. Anecdotally, it seems that, while most organisations have a risk management function and certainly consider internal control issues, not all boards have had the effective management of their companies' risks firmly on their own agenda. In some cases, the board has looked at the Turnbull review exercise and the register of key risks on an annual basis and pretty much left it at that, whereas the audit committee may have overseen risk, but with a focus on internal control. Even in circumstances where risk has been considered, much of the focus has been on financial risks: however, with the exception of elements such as foreign exchange risks, these are often determined by the non-financial risks facing a company, and the latter may be given inadequate attention by the board.

It does not help that risk management has often been seen as a stand-alone function – and having a risk manager has sometimes meant that other managers assume that someone else is taking care of their risks. In this situation, risk management is inadequately integrated into a company's business processes: it often exists in a silo, and neither oversight nor challenge is sufficiently strong or joined up. It seems that accountability for risk issues is often unclear within organisations. Is it the risk manager or the internal auditor – or, more importantly, what is the line manager's responsibility?

Yes, board engagement with the risk process needs to be strengthened. But this will achieve nothing if the management of risk is not thoroughly integrated into business strategy and processes. It needs to be embedded into all levels of an organisation, in a cohesive and seamless way. This will give the business the best chance of delivering against its strategic objectives on time and within budget, and avoiding loss, fraud and ill-advised corporate ventures. And, with both the Walker review and the new UK Corporate Governance Code underlining the need to strengthen risk management, especially at board level, it is a good time to consider how the governance of risk might be improved.

A seamless approach

The proposed UK Corporate Governance Code states that boards should be 'responsible for defining the company's risk appetite and tolerance'.

But there also needs to be a link between the work of the board and work done elsewhere on risk at a more practical level. Companies need to take a top-down *and* bottom-up approach, which considers and manages financial and non-financial risks in the most appropriate way at all levels. It is important that the board is

assured that the risk process is replicated in a consistent manner throughout all the company's operating subsidiaries.

A key element of the board's role is to ensure that accountability for the effectiveness of this risk process is clear at all levels. It is clear that there needs to be greater emphasis, by most boards at least, on their role as the ultimate owners of risk management. Much has been said about the board's need to determine risk appetite, and there is some uncertainty as to what this actually means. Rather than trying to define this, it may be preferable for boards to discuss examples of the type of risks they are prepared to accept and those which they prefer to avoid. The more specific the examples the board can provide, the easier it will be to measure possible future business opportunities against this risk appetite – and from this a risk policy stating which risks fall within the tolerable range and which do not can be created.

In our experience, it is relatively easy to identify the impacts of risks such as supply chain failure, but more difficult for operating subsidiaries to assess the impact of the more intangible risks – such as those relating to reputational issues. It is in such areas that the board has a vital role to play in providing guidance to operating subsidiaries.

However, in embedding an effective risk process, it is essential that the board does not introduce a risk-averse culture. No one should be suggesting that risk is a negative, which should be avoided at all costs. Business is all about managing risk, not avoiding it, and companies will make no progress without some appetite for risk. After all, the economic climate and the markets for goods and services are constantly changing and organisations need to adapt to this. This inevitably involves an element of risk-taking.

The risk process should also highlight to the operating subsidiaries the key risks that have been identified by the board. But this should be a two-way process – new risks tend to emerge from operational experience, often at operating subsidiary level, rather than just from a head office vision. These need to be flagged up to the risk or audit committee, and ultimately to the board if major.

Once the board has agreed a policy for its risk process, there is a need to consider how often to review it and its outputs. The draft UK Corporate Governance Code proposes an annual review, but there is a need to have a more regular review of the key risks facing a company, and to consider the extent to which they have gained or declined in their prominence for the company.

We suggest this should take place quarterly or even at every board meeting, as every board decision will need to be taken in the light of these risks. Indeed, since the introduction of Section 172 of the Companies Act 2006 (the directors' duty to promote the success of the company), many more boards have started to consider relevant risk issues in every board paper and therefore, hopefully, every board decision. This should be expanded to ensure it covers the elements of the board's key risk impacts.

> Risk reviews should take place at least quarterly.

This approach will give boards a yardstick against which to measure the risk elements of prospective projects and innovations. If something is under discussion which goes beyond the scope of the board's risk tolerance, or on which there is not a clear view, the board will need to discuss it in more detail to form an agreed position on the way forward.

In committee

The board needs to communicate its definition of its risk tolerance and risk policy to the committee to which it has delegated authority for risk oversight. The Walker review proposes that financial services companies should establish risk committees comprised of non-executive directors. Other organisations may choose to do this, or they may use their audit committee – or indeed another type of committee – to oversee risk. Irrespective of the committee selected, the key is for the board to delegate, in clear and unambiguous terms of reference, the work which it expects this committee to carry out. It also needs to specify and see reports it needs to receive from the committee and parameters of issues that need to be flagged with the board directly by the committee at any time.

However, it is also important for the committee to look in detail at how the risk process is being managed by the businesses. It will need regular reports from operating subsidiaries regarding this, and procedure for looking into any concerns. This will mean regular reviews of the risk register, and of how risk is being managed at the committee meeting. The committee will be keen to review the reports of both internal and external audit on risk and will also wish to look at how any concerns raised by both sets of auditors are dealt with by management. The committee may well require a report from the businesses on losses, frauds and threatened legal action above a certain financial level. It is also important to establish how operating companies consider the potential impact of several risks crystallising simultaneously – an area which is often overlooked at an operational level.

Because, ultimately, the board is responsible for a company's reputation – which nowadays represents a sizeable percentage of a company's market capitalisation – the committee needs to pay special attention to information regarding any issue which could damage this reputation.

Operating subsidiaries will also need to be aware of what actions are expected of them. At its simplest, one question is whether they are each expected to keep a risk register at their particular site or feed into a more general register. Unless the sites are very small, it is preferable for each one to keep a risk register. More importantly, subsidiaries should be quite clear who in their organisation is responsible for keeping this register and reporting on it – and how they should involve the subsidiary's line management in the development of a better understanding of the risks that the subsidiary faces.

In this respect, the last piece of the jigsaw is the workforce within each subsidiary or functional department, as the risk management process cannot work successfully without their input. In particular, they need to be aware that they should raise any concerns or issues which could give rise to loss of money or reputation, either through a whistleblowing procedure or informally. The key is that the culture of the organisation should allow for such problems to be raised and discussed constructively: while aiming to be positive and 'can do'. Many companies have unwittingly discouraged the raising of problems and left employees feeling that they are letting the side down and being negative if they raise concerns. This has resulted in many risks, which could have been managed more effectively if raised early enough, escalating to become potentially significant risk impacts.

* * *

Effective risk governance requires a culture that ensures risk is part of a company's business process rather than being outside of it, and hence treated as an isolated exercise. By ensuring the board takes a more active part in ensuring the company's risk processes are embedded throughout the various departments and subsidiaries, it will go a long way to delivering its duty to promote the long-term success of the company.

FURTHER INFORMATION

Board Insight and The Virtuous Circle have jointly developed a Risk Process Review service which evaluates risk governance at all levels of an organisation. For more information, contact Julia Casson at *juliacasson@boardinsight.co.uk* or Tony Hoskins at *thoskins@thevirtuouscircle.co.uk*.