

Groups - Risk Management – Blanaid Clarke

While risk management is not a new concept, the financial crisis has increased awareness of business risks and of the importance of carefully reviewing and managing risks. Initially the Reflection Group considered risk management in the context of Group companies. This was an acknowledgment of the additional risks which arise directly from the group structure. These include risks of contagion, management complexity, risk concentration and conflicts of interest between different parts of the group. However, it became clear that the topic had a wider relevance and the recommendations being made would also benefit other non-group companies.

At the European level, there is limited provision for internal control and risk management systems:

- The 8th Company Law Directive – the 2006/43/EC requires most public interest entities to have audit committees and imposes a duty on audit committees (or alternative bodies) to monitor the effectiveness of companies' internal control, internal audit (if any), and risk management systems. An exception is permitted for SMEs and for subsidiary undertakings where the requirements of the undertaking are complied with by its parent undertaking. This has been described in the *RiskMetrics Study (2009)* as "the Directive's most frequently non-transposed article".
- Recommendation 2005/162 recommends that an audit committee be established (unless the board is small) and that it assist the board in its task to review the internal control and risk management systems and the effectiveness of the external audit process and to ensure the effectiveness of the internal audit function. It also provides that the (supervisory) board should ensure that shareholders are properly informed as regards the affairs of the company, its strategic approach, and the management of risks and conflicts of interest.
- Directive 2006/46/EC on Company Reporting requires listed companies to include a corporate governance statement in their annual report containing "a description of the main features of the company's internal control and risk management systems in relation to the financial reporting process." In the case of a consolidated annual report there should be a description of the main features of the group's internal control and risk management systems in relation to the process for preparing consolidated accounts.
- IAS Regulation (1606/2002) requires publicly traded companies to prepare their consolidated accounts in conformity with international accounting standards (IAS) and international financial reporting standards (IFRS) as adopted by the Commission. The IFRS Regulation requires that the directors' report business review include a requirement to describe the "principal risks and uncertainties" facing the company and its subsidiaries.
- The Transparency Directive 2004/109/EC requires the annual financial report of listed companies to include a description of the principal risks and uncertainties that the companies face.

Following the banking company failures in 2007 and 2008 EU regulation of risk management for investment firms and credit institutions also increased (e.g. through the Capital Requirements Directive and the Commission Recommendation 2009/384/EC on remuneration policies) in recognition of the high systemic risk involved.

In some Member States, statutory provisions go further at least for listed companies. For example, German law requires aktiengesellschaften "to establish a system by which developments endangering the existence of the company can be detected from early on" and Danish and Swedish law requires the board to ensure that the company's organisation is structured so that accounting, cash management and the company's business operation are controlled in a prudent manner.

Many jurisdictions such as the UK and Belgium utilise a balanced approach that combines features of mandatory requirements in combination with best practices and certain others leave detailed risk management matters to national corporate governance codes many of which are applied on a

comply-or-explain basis. The UK Corporate Governance Code (2010) states that the boards of all listed companies are responsible for determining the nature and extent of the significant risks they are willing to take in achieving their strategic objectives. Boards are required to maintain sound risk management and internal control systems. Internal control and risk management extends to all operational activity and is not merely limited to the financial reporting process. These are core principles which listed companies must comply with and report on to their shareholders. The UK Turnbull Guidance advises that "for groups of companies, the review of effectiveness of internal control and the report to the shareholders should be from the perspective of the group as a whole".

While the comply-or-explain principle enjoys the support of regulators, companies and investors, even outside the banking sector, there has been a clearly acknowledged need for improvements in the effectiveness of internal risk management and firm governance. The RiskMetrics survey of investors indicated a perception that disclosure is worst regarding risk management, financial risk exposure, and nonfinancial risk profile. Companies and directors surveyed found that the existing codes have almost no effect on issues linked to risk management from the perspective of strategic scenarios.

Recommendations

At least in the case of large listed groups of companies there is a role for EU law in regulating management and oversight structures. In determining this role, the Reflection Group took into account the fact that the elaborate and costly US Sarbanes Oxley Act did not prevent the financial crisis and that there are therefore limits to what can be achieved by increasing disclosure or substantive obligations relating to risk management. Furthermore, it also accepted the argument that viable companies have a market incentive to engage in all cost-effective risk control devices and that restricting them to *formal* and *verifiable* ones might be seen as unjustified.

The following recommendations are made:

- The obligation in Directive 2006/46/EC to describe the risk management systems should be extended beyond financial reporting to include operational risk and should explain, avoiding boilerplate approach, risk management functions, risk management policies, structures and procedures.
- A general duty should be imposed on directors of large listed companies to take into account the risks of the company and to provide for safe and prudent organisation of its affairs. (For Group companies, responsibility for risk management should be placed upon the board of the parent company.)

In view of the complexity of these issues and the differences in national corporate governance structures, this obligation might be best included in a Commission Recommendation which could be implemented in a Corporate Governance Code. (This is not without its difficulties however. There are differences between Member States as regards the scope of application of the national corporate governance codes, with certain codes applying to companies listed in the relevant Member State, and others only to companies listed and incorporated in the Member State. Where a company is incorporated in one Member State but is listed in another or several other Member States, this may result in situations where several codes are applicable or no code at all. Furthermore, compliance with the Code may not be well monitored and this is something the Green Paper is seeking views on.)

In the Recommendation the of the main features of the relevant internal control and risk management systems might be described and might include: sound administrative, reporting and accounting procedures to identify, measure, monitor and control risk in all entities in the group; policies to identify potential conflicts of interest and monitor their implementation; appropriate

instruments to identify early signs of impending financial weakness; procedures to integrate risk monitoring systems into the company in a consistent way so that the risks can be measured, monitored and controlled at the level of the company, including subsidiaries (and taking into account the nature, scale and complexity of the different risks to which the group and its subsidiaries are exposed); and the identification of a person or committee responsible for risk management with a strong status within the entity and strong reporting lines to the relevant committee.

The Group acknowledged that increasing disclosure would be costly in terms of management time, loss of confidentiality etc. As the European Corporate Governance Forum noted "the wider the types of risk to be addressed and the more extensive the disclosures required, the greater the costs, difficulties and challenges faced by management and those charged with governance". While empirical evidence would appear to suggest that a risk information gap exists, clearly a balance will need to be struck between providing excessively detailed risk disclosures on the one hand and overly generalised boiler-plate statements of risk management policy on the other. Determining the exact nature of the disclosure obligation (both how detailed and of what) is not straightforward. A distinction can be drawn between disclosure of the risk monitoring structure of a particular company which serves to a) ensure that it is in place within the company or b) to enable investors to assess the risks of the company in their overall evaluation of the company. The distinction is thus between disclosure as a) compliance or b) pricing mechanism.)

The European Commission in its Green Paper on Corporate Governance while accepting that it does not seem possible to propose a 'one size fits all' risk management model for all types of companies, stated that it is crucial that the board ensures a proper oversight of the risk management processes. Based on Commission interviews it noted the generally accepted view that the board of directors bears primary responsibility for defining the risk profile of a given organisation according to the strategy followed and monitoring it adequately to ensure it works effectively. It describes as "indispensable" the need to define clearly the roles and responsibilities of all parties involved in the risk management process: the board, the executive management and all operational staff working in the risk function. One of the questions in the consultation thus is whether the board should approve and take responsibility for the company's 'risk appetite,' report it meaningfully to shareholders and ensure that the company's risk management arrangements are effective and commensurate with the company's risk profile.

oOo