

31 August 2010

Dear Sir,

The Institute of Risk Management welcomes the current consultation launched by the European Commission on the 'Corporate governance in financial institutions and remuneration policies' as an opportunity to influence and shape the debate on the development of Corporate Governance best practice in the European Union.

The Institute of Risk Management (IRM) is the world's leading enterprise-wide risk education Institute. We are independent, well respected advocates of the risk profession, owned by practicing risk professionals. IRM passionately believes in the importance of risk management and that investment in education and continuous development leads to more effective risk management. We provide professional qualifications, short courses and events at a range of levels from introductory to expert. IRM supports risk professionals by providing the skills and tools needed to put theory into practice to deal with the demands of a constantly changing, sophisticated and challenging business environment. We operate internationally, with approaching 3000 members and students in over 50 countries, drawn from a variety of risk related disciplines and a wide range of industries.

We have attached, as a detailed appendix, specific responses to a number of the questions raised by the Green Paper.

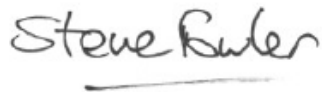
We would however wish to take the opportunity to highlight the key themes that the Committee should consider in reviewing Corporate Governance:

- Rules and regulations are an important but not sufficient element of driving a Board of Directors to sponsor and maintain an enterprise risk management framework.
- A risk management culture can be encouraged but cannot be mandated. However defining clear accountabilities and driving best-practice remuneration policies are positive steps towards such a goal.
- The Chief Risk Officer and the risk function that supports that role holder have a potentially significant contribution to make in

developing a more professional approach to the management and reporting of risk.

- Requiring organisations to make public disclosures regarding the manner in which they manage risks is a powerful tool in encouraging maturing of risk management provided the risk of 'boiler plate' responses is guarded against.

Yours sincerely,

A handwritten signature in black ink that reads "Steve Fowler". The signature is written in a cursive style and is underlined with a single horizontal line.

On behalf of the Institute of Risk Management

Steve Fowler, Chief Executive

Institute of Risk Management
6 Lloyd's Avenue
London
EC3N 3AX

E-mail: steve.fowler@theirm.org
Tel: +44 (0)20 7709 9808

APPENDIX

Corporate governance in financial institutions and remuneration policies consultation

1.6. Should it be compulsory to set up a risk committee within the board of directors and establish rules regarding the composition and functioning of this committee?

The Institute believes that it is highly beneficial for financial institutions to establish a Board-level committee focused on risk and the management of material business risks.

It is important for the effective implementation of enterprise risk management that there is effective high-level sponsorship of risk management. Non-executive directors should be well informed on the material risks facing their business and able to effectively challenge executive management.

A specific Risk Committee would provide a clear message that risk management is not a 'compliance exercise' within a particular institution.

We would stop short of making this provision mandatory for all financial institutions. We believe this type of provision is best implemented by engagement with Boards rather than coercion and would therefore recommend that this requirement be subject to a 'comply or explain' requirement.

1.7. Should it be compulsory for one or more members of the audit committee to be part of the risk committee and vice versa?

Where there is a Risk Committee established, the Institute would see benefits in at least one member of the Audit Committee also sitting on the Risk Committee.

The benefits of such a requirement would be to ensure that there is consistency between the scrutiny given to the management of risks, audit planning and the overall evaluation of internal controls.

Recognising that many smaller financial institutions have access to limited numbers of non-executive directors, there should be no compulsion to share more than one member. Such a move could be counter-productive in encouraging organisations to replicate the membership of both committees and scheduling 'back to back' meetings which would, in effect, be an extended Audit Committee.

1.8. Should the chairman of the risk committee report to the general meeting?

If an organisation established a Risk Committee, the chairman of the committee should have equal status with the chairman of other Board-level committees and report to general meetings where appropriate.

It would be logical for the Risk Committee to provide a separate report within the Annual Report and Financial Accounts of the organisation. This would imply re-organising the Annual Report to ensure that risk management is adequately covered without undue repetition.

1.9. What should be the role of the board of directors in a financial institution's risk profile and strategy?

The Institute believes that the Board of Directors has a central role to play in the development of an organisation's strategy and challenging plans proposed by executive management. The Board should be fully engaged in the consideration of an organisation's risk profile. The risk profile should be an expression of the challenges the organisation considers may arise in delivering its strategic objectives.

The Board should be considered the primary audience for the organisation's risk profile and is there to challenge and hold executive management to account for its management of risks associated with delivering an agreed strategy.

Central to address this issue is how an organisation defines its risk appetite, sets risk tolerance limits and ensures that these are complied with. The Board should have a specific accountability for setting, maintaining and reviewing the risk appetite of the organisation. Executive management should be held to account for any deviations from agreed risk appetites or risk tolerance limits.

These requirements are well expressed in the recent UK Governance Code: "the board is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives".

The Board as a whole should therefore have the skills and experience required to discharge this role of challenge and review.

1.10. Should a risk control declaration be put in place and published?

The Institute believes this could be a positive development but needs to avoid becoming a 'boiler plate' process whereby statements are produced but are worded such that little meaningful information is provided.

Shareholders and stakeholders should understand the strategy of the organisation and the risks inherent in this strategy. In order to achieve business objectives and produce the returns expected by investors and stakeholders, organisations should be able to take proportionate levels of risk.

The Board should be able publicly to articulate the organisation's risk appetite and how it gains assurance that the organisation operates within this appetite. Organisations should be allowed to adopt strategies within different levels of risk associated with them provided these have been understood, challenged and endorsed by the Board.

The Board should be required to articulate the strategy clearly to shareholders and stakeholders and explain how it has considered and addressed the material risks inherent in this strategy. The Board should be required to provide an opinion on the effectiveness of the controls in place to manage these risk exposures within the agreed risk appetite.

1.12. Should an obligation be established for the board of directors to inform the supervisory authorities of any material risks they are aware of?

The Institute believes that such a move would be counter-productive. The majority of regulatory reporting on risk and control gravitates towards a standard format with minimum standards developing quite quickly. This in many cases produces the opposite to the desired effect in terms of communicating less whilst giving the appearance that all is as it should be.

The speed and timing of regulatory submissions are such that this requirement may slow down responses to major crisis events.

The Board has a duty to act if it believes that the organisation is threatened by material risks issues, considered to be beyond the organisation's risk appetite.

The Board should hold executive management to account for its management of material risks and no regulatory process should dilute this accountability.

1.13. Should a specific duty be established for the board of directors to take into account the interests of depositors and other stakeholders during the decision-making procedure ('duty of care')?

The Institute believes that Boards have a broad set of duties towards shareholders, clients and wider stakeholders. Enterprise risk management provides a mechanism for managing significant threats and opportunities facing an organisation and articulating them so that stakeholders can be made aware of them in an appropriate manner.

The sustainability of organisations is best served by ensuring that Boards maintain a balanced view of the objectives of the organisation and think beyond short-term shareholder return. The evaluation of the impact of decision-making on wider stakeholders is an articulation of the establishment of a clear risk appetite framework as outlined in answer 1.10.

The Institute would therefore support a wider 'duty of care' provided this requirement was principles based and allowed Boards sufficient room to interpret its requirements to their organisational circumstances.

2.1. How can the status of the chief risk officer be enhanced? Should the status of the chief risk officer be at least equivalent to that of the chief financial officer?

The Institute believes there is a significant role to be played by senior risk professionals in financial institutions. Recent crises have demonstrated that an independent executive view of the risks facing an organisation is key to management taking a balanced view.

Chief Risk Officers are executive managers and as such should report to either the Chief Executive Officer, or where appropriate to the Chairman of the Risk Committee.

Their day-to-day role is to be adviser and counsellor to the CEO and assist management in better understanding and addressing material risks.

The professionalism of CROs should be considered carefully and addressed proactively. An organisation would not appoint a Finance Director without assuring itself that the role holder was competent and qualified. The same is true of risk professionals. Senior risk professionals should be appropriately qualified and hold membership of professional institutes such as the Institute of Risk Management. We would suggest that in order to achieve a significant improvement in the management of risk across the financial services sector, the appropriate qualifications for CROs must include a detailed understanding of enterprise wide risk management concepts as well as specialist quantitative skills.

CROs need to be empowered where necessary to act as the ultimate 'whistle blower' bringing material risks to the attention to the Board of Directors. In order to have the authority, gravitas and reporting line to the Board, Chief Risk Officers should be able to report independently of management to the Board.

However during a crisis, they have broader responsibilities in overseeing the effective implementation of contingency and crisis management plans and providing independent challenge to decision making.

2.2. How can the communication system between the risk management function and the board of directors be improved? Should a procedure for referring conflicts/problems to the hierarchy for resolution be set up?

The risk function has a critical role to play in communicating material risk information to the Board. This risk function supports the Chief Risk Officer in delivering their role effectively. The risk function holds a position of trust and supports executive management in providing timely and accurate risk information to enable management to make appropriate decisions.

At the same time the Board needs to be able to gain assurance over how material risks are being managed and provide sufficient challenge to executive management.

The risk function is an executive function and therefore supports management in discharging its duties as a 'second line of defence'. Where there is a conflict of interest, this should in the first instance be managed through the Chief Risk Officer's direct access to the Board. Ultimately the risk function may need to seek support from the Internal Audit function in bringing significant problems to the awareness of the Board.

2.3. Should the chief risk officer be able to report directly to the board of directors, including the risk committee?

The Institute believes as noted above that to be effective Chief Risk Officers require the authority to act independently of executive management in exceptional circumstances.

The Chief Risk Officer should be invited to the Risk Committee as a matter of routine, where there is one, as is normal practice with the Head of Internal Audit and Audit Committees.

The CRO should not be placed in a position of deciding what is 'right' and hence affecting the future viability of their career. In order to be effective under circumstances leading to a crisis, the CRO should feel able to deliver difficult messages to the Board in a professional manner.

To this end the appointment and removal of the CRO should be a matter reserved for the full Board.

2.4. Should IT tools be upgraded in order to improve the quality and speed at which information concerning significant risks is transmitted to the board of directors?

The detail of communication tools used by financial institutions should be a matter for executive management. Reporting of risk information should clearly be timely and accurate. The Board should hold management to account on its ability to report effectively on material risks. Tools should be proportionate to the size of the organisation and the risks that it faces.

To mandate reporting requirements would detract from executive management accountability and the role the Board has to challenge.

2.5. Should executives be required to approve a report on the adequacy of internal control systems?

The Institute believes that executive management are ultimately accountable for the management of risk and this response is closely aligned to question 1.10.

The Institute has found that requiring executives formally to report internally to the Board and to be required to provide management assurance and

personally 'sign off' is a powerful tool in ensuring management has truly understood and correctly articulated the issues. Management should be able to demonstrate to the Board that it is operating within the organisation's agreed risk appetite and that risk tolerance limits are being complied with.

It is critical in such circumstances that the Board holds management to account and challenges the reports provided. This will support the Board in making any external disclosures on risk management and effectively creates a chain of assurance.

Organisations should be free to adopt strategies whereby management provide this assurance to the Board provided that the process can be challenged and endorsed by the Board.

The Institute would be pleased to assist further if required in this project and its implementation if required.

*Institute of Risk Management
6 Lloyd's Avenue
London
EC3N 3AX*

*E-mail: steve.fowler@theirm.org
Tel: +44 (0)20 7709 9808*