



EUROPEAN *CONFEDERATION* OF INSTITUTES OF INTERNAL AUDITING

Phil Tarling
PRESIDENT

Carolyn Dittmeier
VICE PRESIDENT

ECIIA European Confederation of Institutes of Internal Auditing
Representative Register
ID Number: 28608726266-79

21st July 2011

Re: Response to the EU Green Paper on ‘The EU corporate governance framework’

Dear Sir/Madam,

The ECIIA (the European Confederation of Institutes of Internal Auditing) would like to thank the European Commission for the opportunity to comment on your Green Paper “The EU corporate governance framework”.

The ECIIA is a confederation of national associations of internal auditing located in 35 countries, including all those of the EU, representing over 35,000 internal audit professionals. As such, the ECIIA is an Associated Organisation of the global Institute of Internal Auditors (the IIA), a professional organisation of more than 170,000 members in some 165 countries. Throughout the world, the IIA is recognised as the internal audit profession's leader in certification, education and research regarding internal auditing. The IIA also maintains the International Professional Practices Framework (IPPF) which includes the *International Standards for the Professional Practice of Internal Auditing* (available in 29 languages), the Definition of Internal Auditing, the Code of Ethics, practice advisories and other guidance.

[\(http://www.theiia.org/guidance/standards-and-guidance/interactive-ippf/\)](http://www.theiia.org/guidance/standards-and-guidance/interactive-ippf/).

Our specific response to questions 11 and 12 as regards board responsibilities over risk management is more extensive in light of the fact that this area is one of the primary areas of focus of internal audit's overall assurance role. Responses to the other questions of the Green Paper are included only in the case that we have a comment.



Preliminary questions

1. Should EU corporate governance measures take into account the size of listed companies? How? Should a differentiated and proportionate regime for small and medium-sized listed companies be established? If so, are there any appropriate definitions or thresholds? If so, please suggest ways of adapting them for SMEs where appropriate.

In general EU corporate governance should take into account the size of listed companies and a differentiated and proportionate regime for small and medium sized listed companies should be established with the objective of facilitating compliance and simplifying management structure. The “comply-or-explain” clause in national corporate governance codes is useful for this purpose.

There are however certain core corporate governance principles and measures that should be applicable to all, and be oriented to clear outcomes.

Criteria for proportionality to be considered are for example turnover, market capitalization, level of international operations and geographical presence, number of employees, level of significance to public social interests. In addition to some useful reference to the Basel II framework and the Eurostat for defining SMEs, many national codes incorporate the concept of proportionality in their rules or comply and explain approach.

2. Should any corporate governance measures be taken at EU level for unlisted companies? Should the EU focus on promoting development and application of voluntary codes for non-listed companies?

The ECIIA does not advocate legislation for unlisted companies. However, the EU should promote the development and application of voluntary codes or guidelines on core principles of corporate governance applicable to all companies, both listed and unlisted, for use at national level.

This takes into account that the stakeholders of a company go well beyond shareholders; corporate governance crises affect also employees, customers, suppliers, lending institution, etc.

At national and European level, Institutes of directors, of internal auditors and of risk managers as well as the primary business associations have been very useful in providing guidance and significant publications. This wealth of information should be referred to in formulating guidance and promoting a voluntary approach towards good governance.



Board of Directors

3. Should the EU seek to ensure that the functions and duties of the chairperson of the board of directors and the chief executive officer are clearly divided?

We believe that the most important point is that the **accountabilities** of key functions must be set out. The clear description of respective roles allows for the identification of excessive concentration of power if there is no appropriate check and balance.

In some countries the optional aggregation of Chairman and CEO is compensated by the presence of a lead independent director. Potential restrictions should in any case distinguish the needs of large listed companies from those of other organisations.

4. Should recruitment policies be more specific about the profile of directors, including the chairman, to ensure that they have the right skills and that the board is suitably diverse? If so, how could that be best achieved and at what level of governance, i.e. at national, EU or international level?

National codes should state that companies should guarantee the right set of combined skills at board level so as to ensure proper piloting of strategy and governance. The EU could promote or make recommendations on needed areas of skills and training. This is not just financial; the combined skills of directors must allow for the oversight function of strategy, risk, audit, control, compliance and reporting. This includes the need for business experience as well as other knowledge and skills. The proper combined set of skills is considered to be significantly lacking in many situations and a partial cause for the unsuccessful governance by boards and audit committees. Thus, mechanisms to promote training and development are encouraged.

Disclosure of qualifications of directors is also considered appropriate.

5. Should listed companies be required to disclose whether they have a diversity policy and, if so, describe its objectives and main content and regularly report on progress?

We agree in general. However promotion of diversity should be made primarily by other communication and training means. Diversity of course goes beyond gender issues (see also point 4). It is of course essential to provide shareholder meetings with proper and timely information about candidates for directorships.

6. Should listed companies be required to ensure a better gender balance on boards? If so, how?

A better gender balance should be promoted through initiatives which take into account the local country environment and with the support of business associations and institutes of directors. Disclosure requirements would enable interested parties to monitor performance in this area.



7. Do you believe there should be a measure at EU level limiting the number of mandates a non-executive director may hold? If so, how should it be formulated?

We do not believe EU legislation is appropriate here, taking into account the existing Commission Recommendation 2005/162/EC.

Limitations for a non executive director should be thus considered in national codes. Guidelines need to emphasise the principle of ensuring adequate time commitment rather than imposing a blanket limitation on the number of mandates. A review process of this by a specific corporate body or function could be useful at the moment of acceptance of the nomination or renewal.

8 Should listed companies be encouraged to conduct an external evaluation regularly (e.g. every three years)? If so, how could this be done?

Listed companies should be encouraged, although not obliged, to conduct an external evaluation periodically. Specialist firms may play a role here. The Quality Assurance and Improvement Programme methodology adopted by the internal audit profession is also a useful reference. Mechanisms applied in some EU countries also offer good reference including self assessments led by the lead independent director.

Additional measures of self assessment on an annual basis are equally encouraged with the central role of the Chairman and the support of the audit committee.

For subsidiary companies, internal audit of the holding company may be attributed responsibilities for internal assessment or guidance of a self assessment process.

9. Should disclosure of remuneration policy, the annual remuneration report (a report on how the remuneration policy was implemented in the past year) and individual remuneration of executive and non-executive directors be mandatory?

10. Should it be mandatory to put the remuneration policy and the remuneration report to a vote by shareholders?

We support disclosure of remuneration and remuneration policy, in promotion of transparency. Remuneration policy helps stakeholders to understand the association between remuneration and long term and short term performance.



11. Do you agree that the board should approve and take responsibility for the company's 'risk appetite' and report it meaningfully to shareholders? Should these disclosure arrangements also include relevant key societal risks?

12. Do you agree that the board should ensure that the company's risk management arrangements are effective and commensurate with the company's risk profile?

We agree that the board should take responsibility for the company's overall risk profile, including 'risk appetite', risk assessment and risk response. We also agree that the board should ensure that the company's risk management arrangements are effective and commensurate with the company's risk profile. (See also previous points on board competencies, accountability and diversity)

Meaningful reporting on an annual basis to shareholders should focus on the clear description of the company's risk management processes. Risk profiles should be disclosed to the extent that it assists stakeholders in investment decisions without compromising commercial aspects.

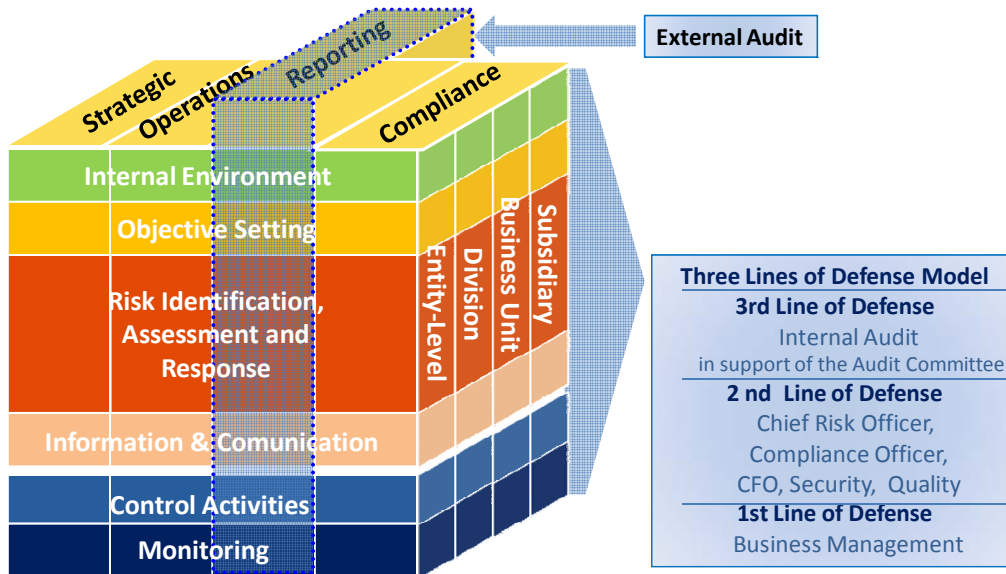
As to societal risks, company adoption of a comprehensive risk assessment model proposed below includes such risks (environment, social, political) as they are an integral part of the framework.

The board should ensure proper oversight of the risk management process. This means approving the type of risks that the company will take and approving the risk profile implied in its strategic plans. It also involves monitoring the system of risk management and internal control to ensure it will be effective at identifying risks and responding to them in accordance with the agreed risk profile.

Especially in large companies, processes for managing risk can be complex and can involve many different people, fulfilling different roles. There is no one single way to manage risks. Therefore, we suggest that it would be helpful if the EU recommended companies to adopt a risk management framework or methodology appropriate for the company and to disclose to their shareholders the framework of methodology they have chosen. There are several such frameworks that can be helpful: the Enterprise Risk Management Integrated Framework of the Committee of Sponsoring Organizations of the Treadway Commission ("COSO ERM" or "COSO2") is a key international example describing the components of a good risk governance framework, and the ISO31000 standard issued by the International Standards Organisation is a key reference for guidance on implementing risk management principles. We believe that EU recommendations should leave the company free to choose the framework it wishes but should encourage the adoption of a framework.

In the next sections we provide an overview of the key elements of the international frameworks that can be useful and of the "Three Lines of Defence Model", which clarifies the roles of controlling and monitoring functions.

International Framework for Enterprise Risk Management (ERM)



Integrated framework - Enterprise Risk Management (ERM)

The benefit of adopting this framework was also suggested in the recent report by the Reflection Group on the future of EU Company Law. A successful implementation of an enterprise risk management model can affect the likelihood and consequences of risks materialising, as well as deliver benefits related to better informed strategic decisions, successful delivery of change and increased operational efficiency. Other benefits include reduced cost of capital, more accurate financial reporting, competitive advantage, improved perception of the company, better marketplace presence and, in the case of public service organisations, enhanced political and community support.

A structured approach to implementing risk management on an enterprise-wide basis is possible with the adoption of the ERM framework and is compatible with ISO 31000, another important reference which provides an internationally agreed standard for the implementation of risk management principles.



The main components of ERM are as follows:

- *Internal Environment* encompasses the tone of an organisation, including the essential “tone at the top” and sets the basis for how risk is viewed and addressed by an entity’s people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
- *Objective Setting* must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity’s mission and are consistent with its risk appetite.
- *Risk identification, Assessment and Response*: Internal and external events affecting achievement of an entity’s objectives must be identified, distinguishing between risks and opportunities. Opportunities are channelled back to management’s strategy or objective-setting processes: risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis. Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity’s risk tolerances and risk appetite.
- *Control Activities*: Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
- *Information and Communication* – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.
- *Monitoring*: the entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

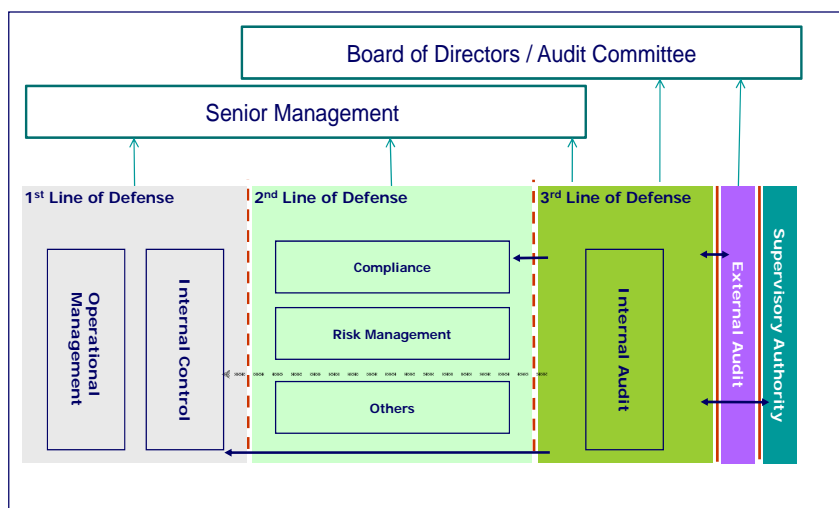
This enterprise risk management framework is geared to achieving an entity’s objectives, set forth in four categories:

- *Strategic* – high-level goals, aligned with and supporting its mission
- *Operations* – effective and efficient use of its resources
- *Reporting* – reliability of reporting
- *Compliance* – compliance with applicable laws and regulations

Three Lines of Defence Model

The ECIIA supports the “Three Lines of Defence” model as a benchmark for future regulatory guidance. This model, illustrated below, is rapidly gaining universal recognition and is consistent with the guidelines already applied in the financial sector.

Three Lines of Defence Model



- **As a first line of defence**, operational management has ownership, responsibility and accountability for assessing, controlling and mitigating risks
- **As a second line of defence**, the risk management, compliance and similar functions facilitate and monitor the implementation of effective risk management practices by operational management and assist the risk owners in reporting adequate risk related information up and down the organisation.
- **As a third line of defence**, the internal auditing function, in support of the audit committee will, through a risk based approach, provide assurance to the organisation’s governing body and senior management, on how effective the organisation assesses and manages its risks, including the manner in which the first and second lines of defence operate. This assurance task covers all elements of an institution’s risk management framework: i.e. from risk identification, risk assessment and response to communication of risk related information (throughout the organisation and to senior management and the governing body).

While the above-mentioned functions operate within the organisation, the **external auditor** contributes as an outside body, providing assurance regarding the true and fair view of an organisation’s financial statements. However, given the specific scope and objectives of their work, the risk information gathered by external auditors is generally limited to financial reporting risks and does not include the manner in which senior management and the governing body are managing/overseeing other (strategic, operational and compliance) risks, and for which the risk management and internal auditing function provide monitoring and assurance, respectively.



This three-lines-of-defence model has been increasingly applied to corporate governance, and particularly risk management, over recent years. The ECIIA finds it a useful tool to demonstrate the different roles in governance and risk management, the interplay between them and how they fit together to provide stronger corporate governance. It forms the basis of a recent paper, jointly issued by ECIIA and the Federation of European Risk Management Associations (FERMA) on “Guidance for boards and audit committees on the implementation of Art 41. 2 of the 8th Directive”. http://www.eciia.eu/system/files/guidance_on_the_8th_eu_company_law_directive_05_10_2010.pdf

Dialogue between control functions and the external auditor is essential. A further role of internal audit is to recommend improvements to the information flow between players, both as to adequacy of communication and efficiency of information.

The Risk Management responsibilities of board and management include¹:

Risk Management responsibilities for the CEO / board:

- Determine strategic approach to risk and set risk appetite
- Establish the structure for risk management
- Understand the most significant risks
- Manage the organisation in a crisis

Risk Management responsibilities for the business unit manager:

- Build risk aware culture within the unit
- Agree risk management performance targets
- Ensure implementation of risk improvement recommendations
- Identify and report changed circumstances / risks

Risk Management responsibilities for the risk manager or risk committee:

- Develop the risk management policy and keep it up to date
- Document the internal risk policies and structures
- Monitor the risk management activities
- Compile risk information and prepare reports for the Board

Risk Management responsibilities for internal audit function:

- Develop a risk-based internal audit programme
- Audit the risk processes across the organisation
- Receive and provide assurance on the management of risk
- Report on the efficiency and effectiveness of internal controls

¹ AIRMIC, Alarm, IRM: *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000, 2010*



It is important to note that the Internal audit role is one of overall assurance, consistent with the Basel Committee reports and best practice (but not limited to the financial sector), and should be fully taken advantage of in order to monitor potential conflicts or inconsistencies or inefficiencies between control functions such as risk management or compliance and operational units.

The internal control system as a whole must be efficient and integrated and the internal audit role should be required by the audit committee or the board to provide assurance in this context. This will provide value by reducing costs from inefficiency and losses on unmanaged risks. The efficiency of the internal governance system, as well as the external financial audit process, will also reduce the need for burdensome measures of outside monitoring bodies.

For the above reasons we believe that the presence of Internal Audit should be included in the requirements covered under the "comply or explain" of corporate governance codes, through recommendation by the European Commission. In general, if the company is sufficiently large to have an Audit Committee, or in the case of Supervisory Boards, then Internal Audit is necessary as an operational arm to that body for global assurance.

The Audit committee in fulfilling its requirement of monitoring risk management, internal control and internal audit as foreseen in Article 41 of the 8th Directive should be called on to consider for each level of defence:

- Adequacy of resources, professional competencies and training
- Outside external evaluations related to quality assurance and improvement programmes, as for example foreseen by the professional standards of the Internal Audit profession

Corporate governance reports which include the main features of the risk management and internal control framework help stakeholders to understand the level in which the Company has addressed risk management, while "boilerplate" responses must be avoided.

Shareholders

13. Please point to any existing EU legal rules which, in your view, may contribute to inappropriate short-termism among investors and suggest how these rules could be changed to prevent such behaviour.

While quarterly reports as well as certain reporting by rating agencies and institutional investors may be oriented to short-termism, we believe that the issue of long term viability should be promoted by other reporting measures which will integrate and progressively transform the aforementioned information.

14. Are there measures to be taken, and if so, which ones, as regards the incentive structures for and performance evaluation of asset managers managing long-term institutional investors' portfolios?

The inclusion of risk indicators in the MBO system in an appropriate and balanced manner, or providing for a correction factor for non compliance issues, would contribute to improving incentive structures which can allow for excessive risk taking. Particular attention should be paid to the different types of institutional investors throughout the European Union. This is not however an area for EU legislation but should form recommended guidance at national level.

17. What would be the best way for the EU to facilitate shareholder cooperation?

While we are not providing a specific proposal, at EU level the promotion of communication processes which increase awareness of the shareholder role is considered useful. Shareholders should be reminded that they have duties in addition to rights.

18. Should EU law require proxy advisors to be more transparent, e.g. about their analytical methods, conflicts of interest and their policy for managing them and/or whether they apply a code of conduct? If so, how can this best be achieved?

19. Do you believe that other (legislative) measures are necessary, e.g. restrictions on the ability of proxy advisors to provide consulting services to investee companies?

We tend to agree. The methodology should be publicly available. Conflicts of interest are of particular concern. EU level restriction for proxy advisors to provide consulting services to investee companies could be considered.

20. Do you see a need for a technical and/or legal European mechanism to help issuers identify their shareholders in order to facilitate dialogue on corporate governance issues? If so, do you believe this would also benefit cooperation between investors? Please provide details (e.g. objective(s) pursued, preferred instrument, frequency, level of detail and cost allocation).

We support in general transparency rules at EU and national level to support in an appropriate manner dialogue on corporate governance.

22. Do you think that minority shareholders need more protection against related party transactions? If so, what measures could be taken?

We tend to agree. The obligation to review related party transactions on the part of the non-executive directors and transparency rules assist here, to be promoted through national corporate governance codes.



Monitoring and implementation of Corporate Governance Codes

24. Do you agree that companies departing from the recommendations of corporate governance codes should be required to provide detailed explanations for such departures and describe the alternative solutions adopted?

We agree. We believe that the “comply or explain” requirements of corporate governance codes should be reinforced to include clear explanation of alternative solutions adopted.

25. Do you agree that monitoring bodies should be authorised to check the informative quality of the explanations in the corporate governance statements and require companies to complete the explanations where necessary? If yes, what exactly should be their role?

We believe that the reinforcement of monitoring the implementation of corporate governance codes and comply and explain practices is needed. At the same time the control by monitoring bodies may be burdensome and perhaps ineffective. Supervisory bodies in some countries have however implemented successfully sample checks of reports which stimulate ‘continuous improvement’ on the part of the listed company.

As the issues involve aspects of internal governance which requires an in-depth knowledge of the company, internal audit’s current role in supporting the Board’s responsibility for proper reporting should also be emphasized.

“Comply or explain” requirements should be reinforced to include clear explanation of alternative solutions adopted. The increase of shareholder involvement whereby the board must illustrate the major aspects of the corporate governance report in Shareholder meetings and the involvement of institutional investors could be useful.

Lastly, it is essential that clear guidelines are provided to companies by national supervisors to ensure a detailed understanding of the objectives and desired content of reporting requirements.

We thank you again for the opportunity to contribute to such an important initiative in favour of sound corporate governance at European level. Please do not hesitate to contact us for any clarifications.

Yours sincerely,

Phil Tarling
President