Hilde Blomme
Director of Practice Regulation
Fédération des Experts Comptables Européens
Avenue d'Auderghem 22-28
B - 1040 Brussels

29 July 2005

Emailed to hilde.blomme@fee.be

Dear Sirs,

Risk Management and Internal Control in the EU Discussion Paper

Thank you for the opportunity to comment on your discussion paper. The European Confederation of Institutes of Internal Auditing (ECIIA) and its member institutes appreciates the work carried out by the Fédération des Experts Comptables Européens (FEE). In particular, we support FEE's efforts to provide guidance to companies and regulators while minimising bureaucratic burdens on them.

Our detailed response to the questions included in your discussion paper is provided in the attached document. However, we should like to draw your attention to three key points:

1 We urge FEE to restate its paper in terms that are unambiguously those of frameworks encompassing risk management and internal control, not just internal control. The possible frameworks are the COSO Enterprise Risk Management – Integrated Framework, the Australia-New Zealand Risk Management Standard and the Risk Management Standard adopted by the Federation of European Risk Management Associations.

2 We believe a great deal of work remains before the European business community has a set of high level principles and criteria it can use to establish, maintain and report on risk management and internal control processes. We should be delighted to assist FEE in continuing this work.

3 We believe that the provision of assurance, firstly by management and then by other assurance providers, is an important part of sound risk management and internal control processes. External or statutory audit is a key assurance provider. However, a professional internal audit activity is also a key player and can provide those charged with governance with objective assurance on the risk management framework and on the management of risks as well as with continuous assistance in setting up and improving such frameworks.

We hope you will find these comments useful and would be pleased to supply any additional information you may require on this or any other related matter. We are quite happy for our response, together with our details, to be considered as part of the public record.

Yours faithfully,

Philippe Christelle
ECIIA past President
Relations with the European Commission

ECIIA - European Confederation of Institutes of Internal Auditing

Koolstraat 47, bus 35 - 1000 Brussels (Belgium)
Tel: +32 2 217 33 20 - Fax: +32 2 217 12 97 - Email: office@eciia.org - Website: www.eciia.org

Fédération des Experts Comptables Européens

Risk Management and Internal Control in the EU
Discussion Paper

Response from the
European Confederation of
Institutes of Internal Auditing

July 2005

INTRODUCTION

The European Confederation of Institutes of Internal Auditing (ECIIA) is a confederation of national associations of internal auditing which are located in countries within the greater European economic area. This includes all of the EU, Eastern Europe, Scandinavia and the Mediterranean basin. With Lithuania and Azerbaidjan joining in October 2004 there are 31 members representing 32 countries and several prospective members waiting to join. There are no individual members, only associations: IIA institutes or chapters. ECIIA is based in Brussels, Belgium.

The global Institute of Internal Auditors (The IIA), of which all our members are part, represents, promotes and develops the professional practice of internal auditing and has 108,000 members in 160 countries worldwide. The IIA sets the *International Standards for the Professional Practice of Internal Auditing*, and the *Code of Ethics*, which all members agree to follow.

ECIIA is run by its members for its members. The General Assembly is made up of a delegate from each member country, meets annually, approves the programme of work and its funding and sets the strategic direction of the Confederation. The Management Board has charge of the day-to-day running of the Confederation, implements strategy and develops policies and programmes, which implement the Confederation's goals and objectives. The Management Board meets at least four times annually.

In preparing this response to your discussion paper, we have solicited the views of all our member institutes. The detailed responses below distil those views and provide the view of ECIIA as a whole.

DETAILED RESPONSES TO YOUR QUESTIONS

1. **Do you agree with FEE that there is a need to promote discussion and evidence gathering to encourage coordination and convergence of the development of risk management and internal control at EU level? If not, please explain. (Section 2.4)**

We agree.

The coordination and eventual convergence of the development of risk management and internal control at EU level should be a key issue for all regulators. Discussions and evidence gathering at this point seem to be the appropriate approach to encourage these developments.

We recommend that the discussions concentrate first on agreeing common definitions that can be used by all members of the EU for terms such as risk management and internal control. Without this step, the discussions would be hindered by the fact that people would be using the same words but meaning different concepts or using different words to mean the same concepts.

2. **Do you consider it appropriate for public policy on risk management and internal control in the EU to focus on listed entities and the needs of their shareholders? Alternatively, do you think that there is a pressing need to deal with issues relevant to a wider range of entities and stakeholders? If so, please explain. (Section 2.4)**

We agree only up to a point that public policy on risk management and internal control in the EU should focus on listed entities and the needs of their shareholders.

The definition of ‘public interest entity’ for the European Commission (EC) includes both listed companies and also financial services companies. The latter should be included in public policy.

Public sector organisations are subject to public policy in these areas through various parts of the EU treaties of accession. Including them and those responsible for their regulation in the debates will help to ensure that the principles of risk management and internal control develop harmoniously between public and private sectors.

Furthermore, the needs of non-listed companies and other organisations should not be neglected. They too need effective risk management and internal control to prosper for their stakeholders and society as a whole. In particular, small and medium-sized enterprises (SME) play an important role in the European economy. Therefore, all these types of entities should be drawn into the debate in order to foster the development of an adequate control and risk management culture, to share best practices developed in the non-listed sector and to encourage the development of principles-based guidance.

However, it is not appropriate at this time to develop public policy and regulations governing those entities, which are not included either by the EC or by their countries in the definition of 'public interest entity'.

3. Do you agree with FEE that the case for introducing any regulation related to risk management and internal control should have regard to: the business case for risk management; the advantages of principles-based requirements; the distinctive features of listed companies; the primacy of those charged with governance; and reasonable liability? If not, please provide details. (Section 3.6)

As long as the regulation being discussed is aimed at improving risk management and internal control processes, we wholeheartedly support FEE's view that the case for introducing such regulation should take into account the five factors:

- the business case for risk management;
- the advantages of principles-based requirements;
- the distinctive features of listed companies;
- the primacy of those charged with governance; and
- reasonable liability

However, the case might be more persuasive if the comments about external audit in paragraph 3.4 were removed. The point is to demonstrate that those charged with governance have primary responsibility, rather than to demonstrate the lesser responsibility of any other group.

We stress that we support FEE's view that regulations should be principles-based, avoiding detailed rules on how companies should implement the principles. Economic analysis exists to show that generic principles-based frameworks, supported by flexible implementation guides, provide an effective basis for successful economic and governmental activity.

We recommend that FEE clarify that the paper is not intended to promote the sort of risk-based regulation that is found in the financial services industry: it is not appropriate for regulation to determine the amount of risk that a company may bear or its risk appetite.

4. Are there overriding principles additional to those identified by FEE in Sections 3.1 to 3.5 that are relevant to risk management and internal control? If so, please explain. (Section 3.6)

There are two additional principles.

A significant aspect we should take into account, when discussing risk management and internal control, is that these issues involve a significant cultural change, including the development of an adequate control and risk culture within companies. In evaluating the introduction of new regulatory requirements, this category cannot be disregarded and standards or guidance should favour the development and the diffusion of a stronger sensitiveness towards these issues. Otherwise, the introduction of new regulatory requirements could determine a further bureaucratisation of processes within organisations, relevant resistance and inertia.

We agree that there is a danger of overreactions that might discourage risk-taking, which is essential to wealth creation. Nevertheless, it is important that decisions concerning risk policies be taken at the right level. According to COSO Enterprise Risk Management - Integrated Framework (ERM-IF) and other control frameworks, risks should be managed to be within the risk appetite of the entity. Therefore the setting of the risk appetite and regular review should be a key responsibility of those charged with governance.

5. Is the matrix for analysis presented in Figure 1 in Section 4.1 clear and useful? If not, please explain why not. (Section 4.4)

The matrix is a useful starting point for discussions but it raises some immediate concerns. It is not really clear what is its purpose. It appears to be taken from the stand-point of outsiders looking into the organisation and, thereby, does not capture all information. It is not principles-based, being fairly prescriptive in its format. It does not appear to encourage embedding risk management activity. It provides a way to compare the legislation and proposed legislation that follows. However, given that it is not a robust model, it runs the risk of providing misleading analysis.

We suggest that the columns are not types of risk but categories of objectives. Since the starting point for risk management should be objectives, then that would be a better label.

Furthermore, FEE has chosen three types. Fairly brief discussion produces many different types that could be used and be equally comprehensive and useful. These include external and internal; safeguarding of assets; separating strategic from operational objectives, particularly since the latter require quite different approaches. We are not suggesting refining the titles of the columns, rather we suggest that a principles-based matrix would not seek to populate those columns but require that management categorise and report on risks in a meaningful way.

The risk management and internal control activities are not complete. Even compared to COSO's ERM-IF, it does not include the evaluation of residual risks. In particular, it makes no reference to assurance and the assurance framework, which is an indispensable part of a strong risk management framework.

Furthermore, it is not clear if the activity "conclude on effectiveness" refers to the entire risk management process or to controls and actions enacted in response of identified risks.

Considering disclosure-related activities, it is not clear if the activity "Effectiveness conclusion" refers to the whole process or to specific risks or both. The problems with the matrix are demonstrated in Figure 4 where the proposed directives' requirement for the audit committee of public interest entities to monitor risk management and internal control is presented as 'conclude on effectiveness'.

We recommend that the matrix be revised to provide a more comprehensive view of risk management and internal control.

6. Is there any need to develop an EU framework for risk management and internal control? If so, how would you address the concerns about resources and benefits identified by FEE in Section 4.2? (Section 4.4)

Therefore, we recommend that work should be done to agree on a common high-level framework for European organisations. This would include definitions, high-level principles and high-level criteria. We do not support the adoption of detailed rules, which dictate how an organisation should implement the high-level principles.

If FEE wishes to base its work on existing frameworks rather than start from scratch, we suggest that it should recommend research that would have three parts. Firstly, a comparison between the main global control frameworks; secondly, a survey of how organisations in Europe adapt these frameworks; and, finally, an extraction of the key elements of the frameworks that are most relevant to Europe. This work should be coordinated with any work to identify high-level criteria for the descriptions of internal control and risk management as envisaged by the proposal to amend the Fourth and Seventh Directives (Question 9).

We recommend that any such analysis should take into account not only control frameworks such as COSO IC-IF but also risk management frameworks. These include COSO ERM-IF, the Australia New Zealand Risk Management Standard and the Risk Management Standard of the Federation of European Risk Management Associations (FERMA), the latter of which has already been translated into 14 languages.

The resources and cost issues of creating and maintaining a new framework are considerable. However, they may be less than the resource and cost issues of having the European organisations each adapting existing frameworks, resulting in inconsistent results for risk management and internal control.

7. Do you agree with FEE's disclosure principles for risk management and internal control set out in Section 4.3? If not, why not and are there additional factors that should be considered? (Section 4.4)

We agree with the disclosure principles in Section 4.3.

We suggest that the first bullet be split into two: it is equally important that the information have intrinsic usefulness and that the benefits should exceed the costs.

We are concerned that statements such as 'Disclosure should be useful to shareholders' could be discussed in greater detailed. This is the nub of the debate and part of the problem in this field of disclosures is that it is not clear what is useful. This is particularly the case since there are many examples were disclosures of risks such as non-compliance with parts of governance codes appear to prompt no particular reaction from investors – until the company's profitability falls.

8. Do you agree with FEE's proposal that there should be a basic EU requirement for all companies to maintain accounting records that support information for published financial statements? If not, why not? (Section 5.6)

A requirement for companies to maintain accounting records that support information for published financial statements would probably be useful.

However, given the diversity in current practices across the EU, it would be sensible to recognise that some companies and some member states may face implementation challenges that will take time to resolve. It would be necessary to explore in more detail the effectiveness of such a requirement and the full range of effects that it is likely to have, including a cost-benefit analysis.

9. Do high-level criteria need to be developed to promote meaningful descriptions of internal control and risk management as envisaged by the proposal to amend the Fourth and Seventh Directives? If so, who should develop the criteria and if not, why not? (Section 5.6)

We agree that high-level criteria are needed otherwise this requirement will become extremely complex and companies will be subject to a great deal of uncertainty.

It is very important that this be done, on the basis of high-level principles, to avoid the development of complicated, bureaucratic requirements.

Given how important this disclosure could be, it will be useful to involve all the relevant bodies in developing the criteria. At a minimum, this would include representatives of the key governance players. This includes directors, internal audit, external audit and shareholders, but could also include investors. Furthermore, the risk management experts must be included to ensure that best practices in this field are taken into account, increasing the chance that we can encourage embedded risk management procedures, rather than having separate systems for disclosure purposes.

The development body should include professional institutions such as FEE, ECIIA, FERMA, company directors' institutes and shareholder or investor organisations.

To a certain extent the work required for the development of high-level criteria will overlap with that required to develop a principles-based framework for risk management and internal control and should be planned with that in mind. (Question 6)

10. What role should regulatory requirements play in promoting improvement in risk management and internal control? (Section 5.6)

Regulatory requirements should focus on providing a common framework for risk management and internal controls. They should identify high-level criteria to promote elements such as consistent reporting, transparency, sharing of best practices, the monitoring role of those responsible for governance and the need for assurance while bearing in mind that excessive regulatory requirements are costly and a deterrent to productive changes.

Regulatory requirements should be recommendations, based on sound management principles and transparency for the stakeholders.

Regulators should avoid defining to precisely what companies have to do and how to do it. They should stay at the level of principles, leaving companies free to decide how best to organise themselves to meet the requirements.

11. Do you agree with FEE's identification of the issues for consideration by listed companies and regulators set out in Section 5.5? Are there any other matters which should be dealt with?

We agree with the issues set out in Section 5.5. However, we have some concerns about Figures 6 and 7 and how they are used.

We recommend that the evolutionary path shown in Figure 6 should be discussed in more detail, particularly with representatives of the risk management profession. It is true that risk events related to financial reporting and compliance objectives may seem easier to identify, quantify and disclose to accountants whose area of expertise these are. However, risk events in other areas are similarly comprehensible to those with expertise in those areas. Therefore, it is not true that the analysis becomes harder as the activity moves to the right. Also, we are not yet convinced that an external report on the effectiveness of risk management and control is the desired end point of the evolution.

As noted above, the matrix repeated in figure 7 is not complete. It omits significant parts of the risk management framework and is static. It should be expanded before being used to recommend future actions.

Some of the analysis of existing legislation is generous to the legislation. For example, many practitioners would argue that the problem with Sarbanes-Oxley S404, as implemented, is that it does not deal with risk, but starts with control objectives. One implication of restricting the scope of work to financial reporting is that the objectives and risks are often felt to be similar for all organisations.

The danger of considering one piece of legislation in isolation is also shown – the fact that Sarbanes-Oxley does not require disclosure of risks but other rules do is not important to the analysis of Sarbanes-Oxley but is relevant to the totality of disclosures available to investors in companies quoted on American stock exchanges.

Also, it would be useful to reflect the interplay of the current proposed amendments to the 4th, 7th and 8th Directives with the earlier amendment that requires companies to disclose:

"at least a fair review of the development and performance of the business and of the position of the undertakings included in the consolidation taken as a whole, together with a description of the principal risks and uncertainties that they face.

"The review shall be a balanced and comprehensive analysis of the development and performance of the business and of the position of the undertakings included in the consolidation taken as a whole, consistent with the size and complexity of the business. To the extent necessary for an understanding of such development, performance or position, the analysis shall include both financial and, where appropriate, non-financial key performance indicators relevant to the particular business, including information relating to environmental and employee matters."

12. What views do you have on the issues for consideration discussed in Section 5.5? (Section 5.6)

We have comments on each of the sections.

Issues related to managing risks

We strongly support your comments on the threats related to 'superimposing risk management and controls on top of existing business practices'. The adoption of risk management systems implies both a cultural and an organizational change; these processes may not be consistent with organisational culture, and their adoption may meet resistance as they which require wide and intense efforts to be managed. Thus, a key

point in this context is to take into account culture and soft factors, which can influence the outcome of the entire process.

A broader framework for risk management and assurance

It is important to have in mind at all times a framework that starts with the objectives of the organisation and ends with a range of assurance that risks to those objectives have been identified and managed according to the organisation's risk appetite. The roles of the players in corporate governance in this framework differ but are all valuable.

This includes management, including risk management, as well as those responsible for governance, often the audit committee. , It also includes assurance providers, primarily external audit and internal audit. Management, internal audit and external audit should all provide assurance. The assurances may have different scopes, so that external audit is likely to be primarily responsible for periodic financial reporting assurances, whereas internal audit and management assurances are more frequent and broader in scope. The assurances also have different degrees of objectivity and independence.

The role of internal auditing in corporate governance, risk management and internal control is critical and internal audit can contribute effectively to the success of most of the proposals contained in the FEE document. Internal auditing remains one of the most important checks and balances available to those in charge of governance. In particular, internal auditing can play a key role to improve cooperation and synergy between the different components of the governance system. ECIIA has issued a Position Paper on Internal Auditing in Europe describing how internal auditors can add value to the governance and risk management processes. FEE should examine this Position Paper and evaluate it with respect to the Discussion Paper and other FEE documents. A copy is attached to this response.

Issues related to disclosures of the overall process

With respect to the opportunity to introduce high-level criteria, see comment to question 9. A primary issue relates instead to "the need to clarity about whether disclosures relate to the process as designed or as operating in practice"; if disclosures aim at supporting investors in achieving a good understanding of companies risk management systems, it is important to require information about the concrete functioning of these systems, otherwise disclosure would be a bureaucratic fulfilment which do not have a real connection with companies' practices.

Issues related to disclosures of management of specific risks

We would like to underscore your comments related to the extension of disclosures beyond specific financial risks.

This will increase the chances of potential liability and reputational damage for directors. There is also a conflict between shareholder's rights to receive reliable and detailed information on business and financial risk exposure and the potential competitive disadvantages and market disruption caused by providing such information.

As the paper suggests, there is a real threat that urging companies to disclose how they manage specific strategic or operational risks may result in superficial reports, designed to comply with regulatory requirements, without providing useful information. Clearly this situation is not consistent with the aims of risk management and internal control systems themselves and the disclosures we are suggesting.

Issues related to disclosures of effectiveness conclusion

It is once more important to take into account the balance between benefits derived from introducing this kind of requirement and the related costs. A key issue is the need not to overburden companies.

13. Do you consider that the current financial statement audit provides adequate assurance to investors in respect of internal controls over financial reporting? Please explain your response. (Section 6.7)

There is a wide variety of opinion across Europe on this.

Where there is a view that current financial statements audit do not provide adequate assurance to investors regarding internal controls over financial reporting, this is related to audit processes and to the specific skills and experience of external auditors. There is also a suggestion that it is not appropriate for external auditors to provide more assurance.

On the other hand, it is felt that the requirements of the new 8th directive will improve the quality of assurance as external auditors report risk management and control issues to the audit committee.

We agree with FEE proposals that external auditors' provision of assurance services in internal control and risk management cannot exceed the responsibilities assumed by those charged with governance. We believe that the ISAE 3000 confirms this approach.

14. Should new disclosures related to risk management and internal control be subject to external assurance? If so, why, and should this be as part of an integrated financial statement audit as in the United States? (Section 6.7)

Until the disclosures have been defined and shareholders have had time to consider what external assurances, if any, they require, it is difficult to speculate on this question.

Assurance may come from many sources. Shareholders may be able to assure themselves about certain disclosures, if they can validate them or their consistency themselves. They may be content with assurances from those responsible for governance, such as the chair of the audit committee or from assurance providers such as the internal audit activity. On the other hand, they may want to receive independent assurance on the consistency of the disclosures with other reporting or on the integrity of the process used to develop the disclosure. It is important to understand what assurances shareholders want before imposing burdens on companies.

After shareholders have decided on what they want assurance, it will be necessary to look at the nature of that assurance and, in particular, the skills, knowledge and experience required to provide them. For example, although professional accountants have the right skills and methodologies for providing assurance on financial reporting, they may not have ones for providing assurance on long-term business risks, strategy and sustainable development.

Therefore, we recommend that before any need for independent assurance is determined, shareholders should review the proposed disclosures and should determine the assurances that they need. Then work should be done to identify the nature of these assurances and the skills required to provide them. Any changes should be introduced on a phased basis, allowing companies, shareholders and auditors to evolve their methods and expectations.

We believe that, whatever the requirements, the regulations or recommendations should encourage the external assurance provider's reliance on the use of work of a professional internal audit activity, complying with the International Standards for the Professional Practice of Internal Auditing and the Code of Ethics of the Institute of Internal Auditors.

The requirements of external assurance of risk management and internal control systems may pose a tangible threat as they may overburden companies with bureaucratic requirements. On the one hand, external auditors could provide more guarantees about the fairness of disclosures' content, which is certainly a positive and desirable result. On the other hand, it is fundamental for FEE to take into account that internal controls and risk management are processes directed to help companies achieve their objectives. Too detailed and burdensome regulations could shift resources from pursuing these objectives to complying with rules. Further, and as the paper highlights, requiring external assurance on risk management disclosures could mean higher costs for companies, which should be carefully compared with achievable benefits.

15. What do you see as the principal priorities in the possible development of new forms of assurance related to risk management and internal control? (Section 6.7)

A key point when speaking about assurance on risk management and internal control processes is to identify how assurance could be provided. Discussion among those charged with governance, auditors and professional bodies will ensure that all viewpoints are taken into account.

We also recommend that audit committees work together with their internal audit activity to improve cooperation with statutory auditors and risk officers, in order to ensure and produce a comprehensive audit of all activities.

Internal audit and statutory audit have different but complementary activities. The two parties should frequently exchange information on the scope of the audit, the audit approach and the findings. Their respective plans should be coordinated.

Although similarities exist in the responsibilities of the statutory auditors and internal auditors, as well as in the area of risk identification and the verification of the existence and effectiveness of internal control, the internal auditor is better placed to provide assurance to the board and to executive management on a range of risks and on an ongoing basis. Moreover, the internal auditor's role includes facilitating improvements of risk management and internal control processes as well as reviewing their effectiveness.

Other detailed points

Section 4.2: the COSO cube is the ERM-IF model, not the COSO IC-IF model as indicated.

Ends