The Association of Insurance and Risk Managers
Telephone 020 7480 7610
6 Lloyd's Avenue, London EC3N 3AX
Facsimile 020 7702 3752
Email enquiries@airmic co uk

27th July 2005

Ms Hilde Blomme
Director of Practice Regulation
Federation des Experts Comptables Europeens
Avenue d'Auderghem 22-28
B – 1040 Brussels

Dear Ms Blomme,

Risk Management and Internal Control in the EU – Discussion Paper

I trust that you have received our response to the above Discussion Paper which we e-mailed to you Please find enclosed, hard copy of our response which is submitted on behalf of the Association of Insurance and Risk Managers (AIRMIC), the Institute of Risk Management (IRM) and the Federation of European Risk Management Associations (FERMA).

Please do not hesitate to contact me should you have any queries regarding our response or if you feel we can provide further information.

Yours sincerely

David Gamble.

David Gamble
Executive Director

Ms Hilde Blomme
Director of Practice Regulation
Federation des Experts Comptables Europeens
Avenue d'Auderghem 22-28
B – 1040 Brussels

Dear Ms Blomme,

Risk Management and Internal Control in the EU – Discussion Paper

We are pleased to submit our comments on the above Discussion Paper. This response was developed and agreed jointly by the Association of Insurance and Risk Managers (AIRMIC) and the Institute of Risk Management (IRM). The response was then reviewed by members of the Federation of European Risk Management Associations (FERMA) and is endorsed by FERMA.
Some brief facts about these three organisations are as follows: -

- **The Association of Insurance and Risk Managers (AIRMIC)**
  The Association of Insurance and Risk Managers was founded in 1963 and represents over 1000 risk managers drawn mainly from large business, charitable and academic organisations in the UK. AIRMIC is dedicated to the development of excellence in Business risk management. AIRMIC's strategic aims include: -
    - promoting the importance and need for excellent business risk management
    - sponsoring and publishing research and guides on business risk management
    - developing core competences in business risk and insurance management

- **The Institute of Risk Management (IRM)**
  The Institute of Risk Management is risk management's professional education body. Established as a not-for-profit organisation, the Institute is governed by practicing risk professionals and has strong links to leading universities and business schools across the world. Recognising that risk management is a multi-disciplinary field, the IRM also works closely with many other specialist institutes and associations and seeks to represent an increasingly broad and diverse set of stakeholders.
  The worldwide membership is drawn from industry, commerce, consultancy and the public sector, and members have backgrounds in many different risk-related disciplines.

- **The Federation of European Risk Management Associations (FERMA)**
  The Federation of European Risk Management Associations brings together the national Risk Management Associations of 12 countries representing Belgium (BELRIM), Denmark (DARIM), France (AMRAE), Germany (BfV - DVS), Italy (ANRA), The Netherlands (NARIM), Portugal (APOGERIS), Russia (RusRisk), Spain (AGERS), Sweden (SWERMA), Switzerland (SIRM) and the United Kingdom (AIRMIC). The above are complemented by a group of individual Risk Managers from Central European countries. FERMA's collective membership of over 4800 individual members represents the major industrial and commercial companies in their respective countries and in

some countries also includes representatives from the educational, health organisations and local authority sectors.

To compile our response, members of AIRMIC and IRM were invited to participate in a discussion meeting. A draft document was prepared that was subsequently adopted by AIRMIC and IRM. The document was endorsed by FERMA after review by its member associations.

We have set out comments on your 15 specific questions posed in the Discussion Paper or, in some cases, have indicated where we believe the questions relate more to accountancy/ financial reporting and therefore are outside the scope of our risk management organisations.

Our debate covered a variety of general issues and concerns relating to the overall approach taken by FEE in its discussion document. Therefore we focussed initially on the ''Key Proposals'' set out in section 1.3. Before providing our detailed comments to the specific questions, we have provided additional comments based on the ''Key Proposals''.

Key Proposals

1. Emphasis should be placed on an overall need for more research and learning from experience to direct developments in risk management and internal control appropriately. It also needs to be widely recognised that profits are, in large part, the reward for successful risk- taking. Therefore the purpose of risk management is to manage risk, including upside risk, appropriately rather than to eliminate it.

We agree, in general, with the points expressed in this first proposal. However we believe that the approach developed in the paper may not be the most appropriate for the following key reasons: -

- The paper appears to assume an acceptance of the COSO framework for internal control. Consequently the emphasis is on internal control rather than taking a more balanced view of risk management and internal control as this key proposal suggests and as does the title of the discussion paper.
- The discussion paper appears to focus on internal control and financial reporting. There is insufficient emphasis on risk management and the various steps in the risk management process. Consequently we believe that this paper does not take risk management forward.
- While reference is made to the more recent COSO *Enterprise Risk Management – Integrated Framework,* it is not used as the framework for the paper. We believe it represents a more comprehensive and balanced approach to risk management and internal control.
- There is no reference to other approaches to risk management (and their related frameworks) which also seek to establish a consistent approach and best practice in this area.
  For example, the Risk Management Standard developed in the UK by AIRMIC, IRM and ALARM and now adopted by the Federation of European Risk Management Associations (FERMA), or the Australian/ New Zealand Risk Management Standard (AS/NZS 4360) (See also comments to questions 1 and 6)
- We agree that there is upside as well as downside risk and that risk management must address both. However COSO implies that ''risk'' is downside, since it uses the term ''opportunity'' when referring to upside. This is at odds with other approaches.

2. There is a need for principles to underpin any regulatory developments in risk management and internal control

We agree with the use of ‘’high level’’ principles which allow organisations flexibility in implementing risk management and internal control and in operating to the principles which may be established. The paper does not set out what such principles might be, although some examples appear to be contained in the text. We believe that principles such as ‘’ comply or explain’’ or ‘’ risk management should be on a cost – benefit basis’’ are the type of high level principles that could be established.
The discussion paper should ensure that key principles are set out clearly.

3. It would be appropriate to reflect existing Member State requirements by introducing a basic EU requirement for all companies to maintain accounting records that support information included in published financial statements.

No comment. This is outside the scope of our risk management organisations.

4. Phasing the introduction of the proposed internal control-related requirements in the Eighth and Fourth and Seventh Directives would be sensible to recognise that some companies and some Member States may face implementation challenges that will take time to resolve.

We agree that this is sensible. The appendices indicate the wide variations in the current status of Member States. There will be similar variations between companies.

5.Proposals as included in the Fourth and Seventh Directives amendments for a description of internal control and risk management systems presuppose the identification of high-level criteria for use by companies in order to facilitate consistent reporting.

We support the idea of high-level criteria to assist in achieving consistent reporting. However, the paper implies that only financial reporting is being considered and therefore we would not comment further.

6. In improving risk management and internal control, companies should follow an evolutionary path over a number of years that recognises the challenges that are involved.

We agree that this is a sensible approach. There will be major variations across EU Member States and indeed between companies in implementing a comprehensive approach to risk management. Therefore, an initial goal may be to achieve a certain standard of risk management across EU Member States in a number of years. However, from a UK perspective, we would stress that there is no ‘’end point’’ as such, since the overall approach always should be one of continuous improvement. Risk management in any organisation should be a continuous and developing process which runs throughout the organisation’s strategy and the implementation of that strategy. It should also be remembered that organisations are dynamic and operate in dynamic environments. Changes in the organisation and the environment in which it operates must be identified and appropriate modifications made to risk management processes.

7. Listed Companies operate in securities markets where pressure to adopt more demanding standards of risk management and disclosure can be reflected through various mechanisms that are proportionate and cost-effective and that can be

effective in bringing about real changes in behaviour. Detailed and prescriptive legal requirements may be less appropriate for this aspect of corporate governance. These mechanisms include: -

- *policies adopted voluntarily by companies*
- *the demands of retail customers of investment institutions*
- *dialogue with shareholders*
- *voluntary or required ''comply or explain'' reporting against voluntary codes; and*
- *ratings applied by external organisations.*

We support this proposal and believe that there is ample evidence that detailed and prescriptive legal requirements can lead to a ''box ticking'' approach which does not further the case of risk management or internal control. The paper already indicates that a Sarbanes- Oxley approach would not be necessary/ appropriate for Europe because of the differences in shareholder rights between European and US companies. Experience is showing already that there are huge costs to companies which have to comply with the prescriptive Sarbanes-Oxley requirements without any significant benefit in risk management. The approach is therefore neither proportionate nor cost-effective.

8. FEE is currently not convinced about the usefulness of introducing across the EU published effectiveness conclusions on internal control over financial reporting as required by section 404 of the Sarbanes- Oxley Act. However, it will be important to take account of the views of investors and companies and forthcoming evidence about the usefulness, costs and benefits of such conclusions to investors as section 404 of the Sarbanes- Oxley Act is implemented.

We agree with this proposal. In addition to the questions over usefulness and cost-benefit, there are also practical issues regarding the assessment of ''effectiveness'' and the reporting of effectiveness conclusions in a consistent way.

9. External Auditors' provision of assurance services in respect of risk management and internal control cannot exceed the responsibilities assumed by those charged with governance.

Please see our comments on Section 6.

10.Auditors should initially work with those charged with governance to identify useful forms of private assurance reporting on risk management and internal control.

It is not clear what is intended by ''private assurance reporting''. Does it refer to consultancy organisations that could provide this type of service or simply to measures that an organisation might use internally to obtain assurance? This should be clarified.

11. In line with the FEE's proposed formalisation of the requirement to maintain accounting records that support financial information, auditors carrying out a statutory financial statement audit should be able to conclude from the audit of the financial statements that such records have been maintained.

No comment. This is outside the scope of our risk management organisations.

12. Further work should be done by the auditing profession to consider how to apply ISAE 3000 to provide external assurance on internal control reporting separate from the financial statement audit.

No comment. This is outside the scope of our risk management organisations.

13. It is essential that auditors' liability fairly and reasonably relates to the consequences of unsatisfactory audit and assurance performance.

No comment. This is outside the scope of our risk management organisations.

Questions for Commentators

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?*

We agree that there is scope for more coordination of risk management and internal control and therefore further discussion and evidence gathering is appropriate. However, at this stage, we believe it should not be assumed that one approach (the COSO Internal Control Framework) is necessarily the most appropriate or that a single approach has to be specified.
In our earlier comments on your first key proposal we indicated that the COSO internal Control framework is not the most appropriate approach, as it does not give the correct balance between risk management and internal control. We mentioned other risk management standards / guidance, some of which are referred to in the paper. (COSO ERM, CoCo, the FERMA Risk Management Standard, AS/ANZ 4360, etc)
We suggest it would be useful to include in the discussion paper a comparison of such standards and the requirements / guidance which they provide on good risk management practice. You have stated that there should be flexibility in approaches to risk management and internal control and that there are dangers in the ''one size fits all'' approach. An organisation could establish a robust risk management system by following and implementing the guidance set out in COSO ERM or the FERMA Standard or the Australia/ New Zealand Standard. There does not have to be only one acceptable approach to achieving the objective of good risk management.
Note: We have made a comparison of the FERMA standard with COSO ERM and the Australia/New Zealand Standard and are happy to make it available should FEE feel it would be helpful.

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?*

We believe that risk management and internal control should apply to a wider range of stakeholders than those related just to listed entities. In some cases, this may be best left to market forces which will require an organisation to demonstrate that it has robust risk management and internal control processes in place. In addition to public listed companies, all organisations which are publicly funded or where there is a public interest should be subject to the same requirements for risk management and internal control.

3. *Do you agree with the 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?

We agree that any approach to risk management and internal control needs to be appropriate, cost – effective, flexible, etc. – points which are made in the discussion paper. However we are not convinced about the need for, or value of, ''regulation'' without the nature of that regulation being defined and without some indication of the extent to which it might be enforced and what penalties might be imposed.

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?*

Section 3 on ''Overriding Principles'' is not clear. For example, 3.2 discusses the advantages of principles based requirements and is as such not a ''principle''.
Section 3 does not make clear what the key principles might be, although it implies that they include considerations such as: -

- comply or explain
- managing risk appropriately
- setting objectives without prescribing rigid rules on how they should be achieved
- allowing for use of judgement
- providing a clear link between risk management strategy and business strategy
- embedding risk management in the business as a decision support tool, not a compliance tool

It is not clear if FEE intends to specify a framework to be used for Risk Management and internal control (or a number of frameworks each of which would achieve the objective of effective risk management and internal control.)

There may be overriding principles that should be considered in addition to your set of implied principles, but it is difficult to suggest what these might be until section 3 is clarified.

5. *Is the matrix for analysis presented in Figure 1 clear and useful?*

We believe the matrix presented in Figure 1 is unhelpful.
It appears to be a corruption of COSO (Internal Control Framework) and does not appear to align with it. The paper should be explicit about which COSO framework is being used. The matrix fails to address the holistic approach to Risk Management and internal control. We suggest it would be better to base any matrix for analysis on the COSO ERM Framework which sets out a more comprehensive framework giving appropriate emphasis to each element of the risk management process.
The matrix presented covers only portions of the complete process. For example, a number of the standards referred to above (including COSO ERM) stress the importance of linking risk management to the organisation's internal environment and its goals/objectives. This important element is not reflected in the matrix.
The matrix is also confusing in that it refers to financial reporting, compliance and operational/strategic as types of risk. COSO ERM makes it clear that reporting, compliance, operational and strategic are the four key categories of objectives.

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?*

We believe there is some merit in having a common framework that could be adopted across the EU. However this would then need to be at a very ‘’high level’’, which might tend to dilute what some Member States and major organisations are doing already on risk management and internal control.
An option, which FEE should consider, is to endorse one or more of the existing Risk Management Standards or frameworks.
The ultimate objective is to ensure that an organisation adopts a comprehensive risk management framework and that it is properly implemented. We believe it is quite feasible therefore to have a number of approaches, any one of which will achieve this objective.
We would question the need to develop another set of requirements/ guidance on risk management and internal control when, for example, FERMA has endorsed that developed in the UK by AIRMIC, IRM and ALARM. This risk management standard has been translated into 14 languages including most European languages and is being used extensively. This standard also seeks to achieve consistency in the use of risk management terminology by using the definitions set out in ISO Guide 73. We have referred to other standards previously that similarly set out a process for risk management.
FEE should also take account of the proposed ISO standard on Risk Management which is about to be developed. Also, a risk management framework is due to be published later this year by the European Foundation for Quality Management. One or more of these approaches could be endorsed by the EU as meeting an appropriate ‘’standard’’ in 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.*

We agree in general with the proposals on disclosure. There are issues regarding the level of detail and complexity of the information provided in disclosures. The paper makes the point regarding differing risk appetites, subjective judgements and difficulties in making statements about the effectiveness of risk management and internal control. What may constitute a significant risk to one organisation may be inconsequential to another.

Linking disclosures to the entity’s general business strategy raises concerns over competition and competitive advantage. Disclosures may be worded in such a bland way that they would give little information of any value to interested stakeholders.

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?*

As indicated in our comments on the key proposals, this is outside the scope of our risk management organisations.

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?*

We support the idea of high- level criteria to promote meaningful and consistent descriptions of risk management and internal control.
These should be developed and agreed by the professional bodies representing Risk Management and Internal Audit.

10. *What role should regulatory requirements play in promoting improvement in risk management and internal control?*

We do not support the use of legislation to promote improvements.
Please see our comments on question 3 regarding ‘’regulation’’ and the need to define regulation in this context.

11. *Do you agree with the FEE's identification of the issues for consideration by listed companies and regulators set out in figure 7 in section 5.5? Are there any other matters which should be dealt with?*

We do not agree with the issues for consideration as set out by FEE in figure 7.
As indicated in our comments on question 5, the matrix is incompatible with the COSO ERM framework and other Standards/ guidance to which we have referred.
Figure 7 gives no sense of an integrated set of activities (or their chronology) which constitutes a comprehensive approach to risk management and internal control.
There are significant omissions such as the need to establish the context for risk management in a specific organisation and the internal and external environment.
These are very important issues for listed companies (or any other organisation) to consider as part of their risk management process. Figure 7 also fails to give any indication that risk management is a continuous process.
Figure 7 gives the impression that the key purpose of risk management and internal control is to provide for reporting and disclosure, rather than to assist an organisation to achieve its business objectives by managing risks effectively.

12. *What views do you have on the issues for consideration discussed in Section5.5?*
In addition to our response to question 11 above, we would make the following points: -

- FEE appears to reject Sarbanes -Oxley as not being appropriate for the EU and we agree with this view. Therefore we question why FEE has included disclosure of effectiveness conclusions given the difficulties which are described in 5.5.4
- The evolutionary process shown in figure 6 is not helpful and does not give the correct balance between risk management and disclosure. Risk management is shown as one step whereas there are three types of disclosure. More elements relating to the risk management process should be added to represent correctly the evolutionary process.
  Given our earlier comments on COSO Internal control and COSO ERM, we do not find the items on the horizontal axis (or the order in which they are placed) helpful. Again, placing financial reporting as the first element appears to put undue emphasis on this versus the other elements of risk management and internal control.
- In the last two paragraphs of section 5.5 (page27) FEE appears to suggest a mechanism by which conclusions on effectiveness could be developed beyond financial reporting and then seems to retract the proposal by indicating that it may never be reasonable to publish effectiveness opinions in relation to operational or strategic risks. This should be clarified.

13. *Do you consider the current financial statement audit provides adequate assurance to investors in respect of internal controls over financial reporting?*

No comment. This is outside the scope of our risk management organisations

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?*

No - as new disclosures related to risk management are not intrinsically auditable. Linking new disclosures to an integrated financial statement audit potentially would restrict risk management to those issues which are auditable and therefore dilute the risk management message.

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?*

We believe that the key consideration in relation to any new form of assurance should be – what does the shareholder (or other stakeholder) want to be assured about? This is likely to be the whole risk management and internal control process. Therefore the stakeholder would want to be assured about: -

- What risk management process is in place
- The robustness of the risk identification and risk assessment
- The robustness of risk mitigation and internal control activities
- That the process is embedded in the day-to-day management of the organisation
- Etc.

This concludes our response to the Discussion Paper and we trust that our comments will be of interest and are helpful.

On behalf of:

The Association of Insurance and Risk Managers (AIRMIC)

The Institute of Risk Management (IRM)

And

The Federation of European Risk Management Associations FERMA)