KPMG LLP
1-2 Dorset Rise
London EC4Y 8EN
United Kingdom

Tel +44 (0) 20 7694 8082
Fax +44 (0) 20 7694 8096
DX 38050 Blackfriars

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

Our ref tc/815

29 July 2005

Dear Hilde

Risk Management and Internal Control in the EU: A Discussion Paper

We welcome the opportunity to respond to the Discussion Paper *Risk Management and Internal Control in the EU***.**

We congratulate FEE on producing a very timely Discussion Paper given the European Commission's intention to require companies to include within their annual report a description of the company's internal control and risk management systems.

We are generally supportive of proposals which call for more transparency including increased dialogue with shareholders and 'comply or explain' reporting against corporate governance recommendations.

Furthermore, we agree that there need to promote discussion and evidence gathering to encourage the development of risk management and internal control at EU level. In this regard we would commend to FEE the work of the Turnbull Review Group which, before considering any enhancements to the UK guidance on internal control, gathered evidence from a significant proportion of the UK market, including listed companies representing 56% of the total market capitalisation of UK listed companies on the London Stock Exchange's Primary Market; institutional investors that are between them responsible for funds under management in excess of £2,350,000 million, and many major accountancy firms and representative bodies.

Finally, the question of introducing across the EU published effectiveness conclusions on internal control over financial reporting (as required by Section 404 of the Sarbanes Oxley Act) is a fraught area – and certainly not a question to be answered before taking account of the views of investors, companies and others.

For all its difficulty, we believe that some form of public reporting by directors on internal controls is needed since it both informs investors and increases the consideration given by directors to the systems of internal control and to the major risks faced by companies. However,

we are not convinced that public reporting on the effectiveness of internal controls over financial reporting is an appropriate model for Europe.

In part this is because a requirement for a statement that processes are "effective" would lead to expensive testing and verification work to a low level of detail and we do not consider the benefit of such a statement to shareholders would be sufficient to recommend that it should be required. Furthermore, we are concerned that such a statement might result in a focus on compliance rather than substantive assessment and management of risk. In this regard, we believe that it is all material internal controls and the management of all risks that is important, not merely internal controls over financial reporting.

* * *

Our comments and recommendations relating to the specific questions posed by the consultation are set out in the attached appendix.

If you would like to discuss any of these matters with us please do not hesitate to contact Timothy Copnell on 020 7694 8082.

Yours sincerely

Timothy Copnell
Director

Appendix

Response to specific questions raised in the Discussion Paper

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 support discussion of risk management and internal control at the European Governance Forum, but we do not believe that the introduction of regulatory requirements is necessarily appropriate in this area. As discussed later, we support the implementation of a high-level and principles-based approach to risk management and internal control within the context of the "comply or explain" framework.

Furthermore, we do not believe that national initiatives in this area have hindered the integration of capital markets within Europe. Rather, the pioneering work carried out in certain member states has been instrumental in driving good governance and risk management practice throughout Europe.

We firmly believe that any steps to encourage coordination and convergence of the development of risk management and internal control at EU level should be based on proper evidence about the likely costs and benefits and the experience gained from introducing various measures at the national level. Such research has recently been carried out in the UK by the Turnbull Review Group which, in July 2004, was invited by the Financial Review Council to review the impact of the Turnbull guidance on internal control since its introduction in 1999, and to consider whether it needed to be updated.

The evidence gathered by the Review Group, which can be found at [www.frc.org.uk] represents the views and experience of a significant proportion of the UK market, including listed companies representing 56% of the total market capitalisation of UK listed companies on the London Stock Exchange's Primary Market; institutional investors that are between them responsible for funds under management in excess of £2,350,000 million, and from many major accountancy firms and representative bodies.

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 agree that any regulation, recommendations or guidance drawn at an EU level should focus on listed entities and the needs of their shareholders. The primary duty of directors is to act in the long-term interests of shareholders, however, we accept that this can be achieved only by having regard to the other relationships on which the company depends -

such as those with employees, customers, suppliers and the community, as well as to the impact of business decisions on the company's reputation and the environment.

As such, consideration of what approach to risk management and internal control might better align the costs and benefits should be judged by the yardstick of what is in the best interests of shareholders - what do shareholders want to know about the risks facing a company and the quality of the company's internal control system.

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?

In the absence of appropriate evidence (see question 1) we are not convinced of the need to include any 'requirements' or 'regulation' in this area. Rather, we believe that a high-level and principles-based approach to risk management and internal control within the context of the "comply or explain" framework can have a lasting positive effect on the integrity of companies' systems of internal control and risk management. In our view, a more prescriptive approach would increase the pressure for a formulaic 'tick box' compliance approach and a focus by directors on compliance rather than the substantive assessment and management of risk. Such an approach would not be helpful either to companies or their shareholders.

Notwithstanding the above, we fully support the consideration of 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 in the development of any Recommendations or guidance in the area of risk management and internal control.

4. **Are there overriding principles additional to those identified by FEE that are relevant to risk management and internal control?**

Whilst we support the overriding principles identified by FEE as relevant to risk management and internal control, there are also some broader concerns that should be considered when developing guidance in this area:

- the ability of investors to make better informed decisions in pursuance of their investment strategies;
- improving public confidence in corporate reporting and governance;
- the balance of costs and benefits;
- the ability of companies to recruit non-executive directors or supervisory board members; and

- the perceived attractiveness of listing.

5. Is the matrix for analysis presented in Figure 1 in Section 4.1 clear and useful?

The matrix presented in Figure 1 can provide a useful high-level summary of the control and risk management activities of a company, or the requirements/recommendations of regulation/guidance.

On a matter of detail, for clarity we would prefer the term "control, communication and monitoring activities" to "respond".

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?

While there may be a place for high-level principles set at an EU level, we do not believe there is a need to develop an EU framework for risk management and internal control. Such a framework would simply add an additional layer between international principles and national codes/guidance and regulation. This is consistent with the conclusions draw by the High-level Group of Company Law Experts chaired by Jaap Winter on whether there should be a EU Code of Corporate Governance.

Furthermore it is not clear what benefits a new framework would add to the existing frameworks developed by CoCo, COSO and Turnbull – all of which are already globally accepted frameworks.

7. Do you agree with FEE's disclosure principles for risk management and internal control? If not, why not and are there additional factors that should be considered?

Disclosure is a key element of effective corporate governance. Its purpose is to ensure shareholders have sufficient information to enable them to form a view on a company's governance as a basis for exercising their rights and responsibilities; and to encourage boards and executive management to discharge their responsibilities with care.

We support the disclosure principles identified in the discussion paper, but wonder whether explicit reference should be made to the need for disclosure to be 'company specific'. Anecdotal evidence suggests that all too often disclosure in this area can be generic, bland and anodyne.

Of course, one of the challenges is to provide meaningful statements on internal control and risk management without disclosing information that is considered commercially sensitive. This issue of commercial sensitivity may need to be addressed within these principles.

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?

We would not object to the introduction of a basic EU requirement for all companies to maintain accounting records that support information for published financial statements. Such requirements already exist in several member states.

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?

In the absence of appropriate evidence to the contrary (see question 1), we are not convinced of the need to establish high-level criteria to promote meaningful descriptions of internal control and risk management. In our experience, companies have had little difficulty in meeting the expectations of the Turnbull recommendations which are similar, but not identical, to those proposed by the amendments to the Fourth and Seventh Directives.

If criteria were to be established, we would wish to see them set at the highest level, for example:

- A summary of how the principal risks (disclosed as required by the Modernisation Directive) are managed.
- A summary of the process by which the board assesses the effectiveness of the system of internal control
- A statement that there is an ongoing process for identifying, evaluating and managing the principal risks and uncertainties facing the company
- An acknowledgement that the board is responsible for the company's system of internal control and for reviewing its effectiveness
- An explanation that the system of internal control is designed to manage rather than eliminate the risk of failure to achieve its business objectives
- An acknowledgement that no system of internal control can provide absolute assurance against material misstatement or loss

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

As discussed above, we believe that regulatory requirements should be applied with a light touch. It is appropriate for certain minimum standards to be addressed by legislation, most notably the area of responsibility and transparency/disclosure. However, we would resist applying the rigidity and brittleness of regulation to how risks are actually managed.

A high-level risk-based approach provided within the context of an inherently flexible 'comply or explain' framework allows emphasis to be placed on what the board consider to be the key risks facing their particular business and the appropriate control infrastructure. The alternative, a 'one size fits all' framework or a uniform set of rules, would not be applicable in all cases.

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

We agree that the areas identified for consideration in section 5.5 are the key issues of concern for companies and shareholders.

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

Figure 6 is successfully illustrates the escalating difficulty faced by management in both managing risk and in disclosure and we support the assertion that in improving risk management and internal control, companies should follow an evolutionary path. However, we believe it is wrong to suggest that published effectiveness conclusions are best practice or even desirable.

For all its difficulty, we think that some form of public reporting by directors on internal controls is needed since it both informs investors and increases the consideration given by directors to the systems of internal control and to the major risks faced by companies. However, we have never considered it appropriate for directors to report publicly on the effectiveness of control due to:

- the difficulty in defining 'effective', especially in the context of the wider, non-financial, aspects of control. Deliberations over the meaning of the term 'effective' have for too long been a distraction from the real corporate governance debate;
- the potential creation of an 'expectation gap'; and
- the potential for increased litigation and liability leading to inappropriate process and cost

We believe that concerns about liability will encourage an overemphasis on documentation and procedural matters and consequently a significant increase in costs – both monetary and management time – without significant benefits flowing to investors. This has been widely reported in the context of Sarbanes-Oxley – which deals with the relatively narrow area of internal controls over financial reporting.

Turning to the issues surrounding the disclosure of the risk management process, we believe that investors would be keen to understand each company's risk appetite and whether or not it had been exceeded. Risk appetite is, of course, notoriously difficult to quantify and articulate. Nevertheless, we believe meaningful information can be provided to shareholders in this area through disclosure of the key risks facing the organisation, the

high-level procedures designed to provide effective internal control, and a summary of the process the board has applied in reviewing the system of internal control. In effect, the *risks*, the *controls* and how the system of controls has been *reviewed* by the board.

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

Without a full understanding of investors' expectations, we are unable to determine whether the current financial statement audit provides *adequate assurance* to investors in respect of internal controls over financial reporting.

Of course, the purpose of the current financial statement audit is not to provide explicit assurance as to the effectiveness of internal control over financial reporting; however, it does, in the UK, enable auditors to form an opinion as to whether proper accounting records have been kept and whether the accounts are in agreement with the accounting records and returns. This should in turn provide some comfort for investors.

Furthermore, the existing work performed by external auditors on internal financial control, and the subsequent dialogue with the board and management report, provide auditors with the opportunity to make common sense suggestions to management and those charged with governance.

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?

We strongly believe that the external auditors' provision of assurance in respect of risk management and internal control can not exceed the responsibilities assumed by the board. Therefore, external auditors can not, and should not, provide assurance on disclosure beyond that made by the board. Furthermore, the perceived benefit of public reporting by external auditors must exceed the costs - judged by the yardstick of what is in the best interests of shareholders.

Consistent with our earlier remarks around published effectiveness conclusions, we believe the external auditors remit should be limited to carrying out high-level procedures around veracity of objectively verifiable statements set out in the board's "description of the company's internal control and risk management systems" – essentially limited assurance engagements. Any extension beyond this requirement to provide an opinion on either the effectiveness of the system of internal control or the propriety of the process used to carry out such a review would, in turn, significantly increase the burden placed on the board without any significant benefit for investors. Furthermore, in managing their own risk, auditors will quite properly seek 'audit' evidence before reporting publicly on internal control. This will inevitably lead companies to develop auditable processes, documentation, additional bureaucracy, and divert management time from running the business.

None of the above comments should be taken as precluding reasonable assurance engagements where the external auditors report privately to the board.

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?

The principal priorities in the possible development of new forms of assurance related to risk management and internal control are:

- Reform of auditors' liability such that liability fairly and reasonably relates to the consequences of unsatisfactory audit or assurance engagements.
- A full study, based on proper evidence, about the likely costs and benefits and the experience gained from introducing various measures at national level.