

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

9 August 2005

Dear Sirs

**RISK MANAGEMENT AND INTERNAL CONTROL IN THE EU - DISCUSSION PAPER**

We welcome the opportunity to participate in this consultation by FEE. This response is submitted on behalf of the PricewaterhouseCoopers' member firms in Europe.

We commend the significant work that FEE has done to summarise current practices and requirements in Europe and the US, and to stimulate the debate.

This consultation is timely, as the measures identified in the European Commission's 2003 Action Plan on Corporate Governance are beginning to be reflected in requirements and recommendations. The timing is also important because of the learning experience from applying the Sarbanes-Oxley Act in the United States, and the fact that EU-based foreign private issuers will have to comply with these requirements from next year.

Our specific comments on the questions in the discussion paper are set out in the attached Annex. In this covering letter we set out some broader observations.

**Evaluating different approaches**

We support the principle, mentioned in the paper, of board accountability for the preparation of financial and other information provided to shareholders. We also support the establishment by companies of effective systems of risk management and internal control. These are fundamental building blocks for maintaining public trust in the corporate reporting process.

At the same time we are aware of the extent of diversity in the EU Member States – countries have differing business cultures, differing legal traditions and, notwithstanding the implementation of the Internal Market initiatives, are at different stages in the development of their market economies. The result is that, in some countries, there is much to do in this area of corporate governance.

It will take some time for a consensus view to emerge in Europe of how matters related to risk management and internal control in companies should best be reported. It is important that the debate takes place in an informed way. The objective should be to evaluate the experience of applying different models, and take the best from different approaches. For example, there has been much discussion in the media of the costs of applying Section 404. At the same time, as indicated at the recent SEC roundtable, some companies that have implemented 404 have found real benefits - for instance they have found that maintenance work was necessary to bring their controls up to the required standard, even where they had previously considered their control environment to be strong.

We note Internal Market Commissioner McCreevy's comment that 'Better regulation does not stop at Europe's borders', made in the context of the recent announcements about convergence of market regulation by the US and EC authorities (for example the intention to drop reconciliation requirements for financial statements by no later than 2009). He expressed a desire to work with the US to achieve similar success in other areas such as corporate governance.

Companies listed on different markets should not be required to establish duplicative or inconsistent processes to satisfy different requirements. Ultimately, the goal should be to have a high-quality, global standard for reporting by management on internal control, in the same way as for convergence of accounting and auditing standards. But the 'ideal' global standard is not necessarily any of the models currently applied – it may be a blend of current approaches, which will be developed in the light of further debate and experience.

## **Clear objectives for internal control reporting, focussed on investor needs**

The proposed revisions to the EC 4<sup>th</sup> and 7<sup>th</sup> Directives include provisions for companies to disclose '*a description of the main features of the company's internal control and risk management systems in relation to their financial reporting processes*', but the proposals are insufficiently clear about the objectives of such reporting.

In our view the giving of disclosures on internal control should not be viewed as an end itself. It should be clear that the purpose is to assist investors and other interested parties in understanding the company's attitude to risk and how the company has policies, procedures and controls in place to identify, assess and manage risks. Three key considerations that flow from this are:

- The level of information that is relevant for the markets and which should therefore be made public
- The level of information that is needed at a board and managerial level
- The extent, if any, to which this information should be examined by auditors.

Investors' needs are not focussed solely around financial reporting information. The market relies upon many different types of data (including non-financial information included in company announcements) and thus needs to know that if it has been subject to appropriate controls and review. The principles of board accountability and responsibility for effective risk management and internal control should therefore apply equally to non-financial information, and should embrace wider operational controls, not just financial controls.

We believe there needs to be a wider debate about these issues involving all interested parties – management, boards, auditors, investors, other users of company reports and regulators. We look forward to the roundtable being organised by FEE later this year, at which these issues can be discussed.

### **Information for market decision-making**

It is easier to obtain views on information the market currently receives, rather than assess what additional information market participants would find most useful. For example, research by MORI in 2005 found that, although a third of respondents believe that companies applying Section 404 deliver better information in a more transparent way, only one in ten considers that 404 reduces investors' overall risk. Would disclosures focused around explaining risks and how those risks are addressed provide investors with more useful information?

Commentators have suggested that an unfortunate side-effect of the current environment is that companies have become unduly risk-averse. More internal company resources are devoted to compliance activities, and fewer to identifying business opportunities where the risks can satisfactorily be controlled and managed.

The capital markets are better served, those commentators argue, by companies disclosing the policies and procedures they have implemented to mitigate business risks and how identified problems have been dealt with, rather than by 'pass/fail' conclusions on the effectiveness of internal controls. As noted in our response to question 7, such conclusions often do not provide helpful qualitative information and can be misinterpreted by users.

### **Inherent limitations of controls reporting**

A further important consideration is the need to recognise that formal internal control reporting requirements are no guarantee against corporate failure, or against fraud. There is no evidence to suggest that, had formal internal control reporting or disclosures been in place at the time, that recent high-profile corporate failures would have been avoided. Businesses seldom fail because of poor controls at the detailed level. Where there is collusive behaviour by the highest levels of management, no formal internal control system or reporting regime will be able to prevent fraud. This needs to be clearly brought out and understood in the debate about the objectives of internal control reporting in Europe.

## **Cost-benefit considerations**

We agree with FEE that any proposals for controls reporting need to be considered carefully from a cost–benefit perspective. Such an exercise is not straightforward, since the incremental costs are relatively easy to identify, while the benefits are much less easy to measure. However, in assessing market perceptions of the costs and benefits, all relevant evidence arising from applying different controls reporting regimes (such as the UK Turnbull and US 404 frameworks) should be collated.

In particular, it will be important to await the evidence from the second year of implementation of Section 404 in the US, when many of the ‘start-up’ costs of first-year implementation will have been absorbed.

## **A European model?**

The practical issues of identifying business risks, developing and agreeing a company position with regard to those risks, and designing and implementing controls are not unique to European businesses. They provide similar challenges to companies the world over. Developing a set of basic principles to drive convergence on internal control reporting across Europe and more widely does not mean that a European framework on internal control needs to be developed.

The COSO Integrated Internal Control framework is already generally accepted and widely used around the world – indeed it forms the bedrock for the ‘principles-based’ Turnbull reporting framework in the UK, as well as the more detailed approach under Section 404. Our view is that COSO should continue to form the basis for the control processes and reporting *within* companies. The issues for debate are what form of external reporting is desirable, and whether there should be differential external reporting between countries, or whether a common pan-European approach should be taken.

We believe principles for internal control reporting by companies in Europe should be established through consultation with market participants, and then requirements and guidance established for companies and their managements.

## **External assurance**

As auditors ourselves, we believe it should be left to others to evaluate and conclude on the extent to which auditors should be involved in reviewing and reporting on the controls assertions made by management. However, as discussed above, such an evaluation should be made with the benefit of all available evidence. Relevant factors might include:

- Whether investors place a premium on management assertions that have been assessed by auditors, as opposed to those that have not.
- Whether companies disclose more control weaknesses prior to the auditors’ involvement or subsequently (it would be interesting for example to contrast US companies’ s302 and s404 disclosures).

As discussed in our response to question 13, it should be made clear that the audit of financial statements is not designed to provide *specific* assurance on internal controls. The auditor's consideration of internal control in relation to a financial statement audit is entirely different to that needed to give assurance on an assertion made by management on its controls.

Auditors *can* provide assurance on internal controls, but this will depend on the nature of the subject matter to be evaluated, the auditor's experience, and whether there is a framework of established criteria by which to make an evaluation.

-----

Our specific comments on the questions in the discussion paper are set out in the attached annex. In this covering letter we have outlined the key issues we consider to be important: We believe action is needed to address investors' expectations of the internal control of European companies. There should be a debate involving all interested parties about the level and type of information that is needed by the market and by boards and management, and whether that information should be subject to independent, external review. The debate should be informed by available evidence and research from experience with different models, and should embrace all types of information reported to the market, not just financial. This consultation by FEE is a valuable first step in that debate.

We would be happy to discuss these issues further with you. If you have any questions regarding this letter, please contact Ian Wright (+44 20 7804 3300) or Graham Gilmour (+44 20 7804 2297).

Yours faithfully

PricewaterhouseCoopers LLP

**Responses to questions in the FEE Discussion Paper ‘Risk Management and Internal Control in the EU’**

**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.**

Yes. This is an important debate and it will be critical to obtain as much evidence and to involve as many interested parties as possible.

**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?**

We believe that public policy on risk management and internal control should be considered from the perspective of the public interest (that is whether it is in the interests of external investors or other third parties whose money or capital is ‘at risk’). We therefore consider that the focus should be on public interest entities, including listed companies and financial institutions.

**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.**

Yes. We believe that all national requirements should be focused on these five principles, in order to drive convergence around high-quality approaches to internal control.

**4. Are there overriding principles additional to those identified by FEE in sections 3.1-3.5 that are relevant to risk management and internal control?**

No.

**5. Is the matrix for analysis presented in Figure 1 in section 4.1 clear and useful? If not, please explain.**

Yes.

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

There is no need to develop an underlying framework for risk management and internal control in the EU, since this is already provided by the COSO framework which is generally accepted and widely used. The specific approaches adopted in some countries, for example the Turnbull guidance in the UK, are in most cases still founded on the basis of COSO. However, there should be greater discussion and convergence in Europe around what gets *reported*, and to whom.

**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?**

Yes – these provide a good starting point. We believe the key is to have a system of controls that complement and support the company’s attitude to risk. The focus on providing conclusions on controls effectiveness is misplaced, since such pass/fail conclusions do not provide useful qualitative information - the reader has no means of discerning those companies that apply the internal control framework comprehensively from those that apply it only superficially. Also, such conclusions need to be carefully worded otherwise they have the potential to be misunderstood – no company could give a statement of 100% effectiveness in application, and the credibility of that conclusion will be undermined by the first problem that is discussed in the public domain, however minor.

The focus should, instead, be on explaining, in the light of the company’s attitude to risk, what policies and procedures are designed to be in place to identify, assess and manage risks. This may require more effort to be directed to developing a general framework for business risk management with clear criteria for reporting (for example in relation to definitions, materiality, how to deal with deficiencies, etc.)

A further option not fully explored in the FEE paper is giving conclusions on the design effectiveness of internal controls, rather than on their operation.

**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?**

Yes, to the extent that this is not already provided through national law in Member States. However, we question whether the scope should be limited to simply accounting records. For example, what records should be maintained by companies to support announcements to the market about price-sensitive non-financial information (such as exploration finds for a minerals extraction company, amount of retail space for a supermarket group, or passenger load factors for an airline)? This information is equally market-sensitive to financial information and should attract a similar level of board accountability and responsibility.

**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 4<sup>th</sup> and 7<sup>th</sup> Directives? If so, who should develop the criteria?**

Our understanding is that the descriptions in the amended Directives may relate only to controls over the financial reporting process. However, to ensure consistency, it may be desirable to have a uniform understanding of what controls and risk management systems mean in this context. The only organisation that can issue authoritative guidance on this is the European Commission itself, on the basis of appropriate advice.

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

Any principles developed at EU level should focus attention on the internal control issues that should be reported, and to whom.

**11. Do you agree with 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?**

Yes.

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

Please refer to the issues discussed in our covering letter.

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

We believe that this question should be answered primarily by investors, not by the auditing profession. However, we disagree with the premise in the question, as the audit of financial statements is not designed to provide specific assurance on internal controls (the language used by auditors in their audit reports under the revised ISA 700 makes this clear). The auditor considers internal control relevant to the preparation and presentation of financial statements in order to design audit procedures appropriate to be able to report on those financial statements. This is entirely different from the process that an auditor would have to follow in order to give a Section 404-type attestation or specific assurance on an assertion made by management on its controls.

**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 US?**

See our response to question 13 and also the comments in our covering letter.



**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?**

As discussed above, the priority is to develop a consensus on what should be reported and to whom. This should be evolved by the market, rather than imposed by regulation, although regulators can act as a conduit for the market to ensure consistency of reporting.

The IAASB has developed International Standard on Assurance Engagements (ISAE) 3000 which provides a basic framework for conducting assurance engagements on non-financial information (such as controls processes over financial information, as distinct from the financial information itself). Once there is a broader consensus over what information should be reported, it may be appropriate to supplement the basic principles and essential procedures in the IAASB standards with further guidance on specific topics.

Additional guidance may be necessary in order to clarify, for example, materiality, the level of evidence required, format of reporting, etc.