R O B E R T J. M A R T I N

12 August, 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

As I am currently at home recovering form surgery to a shoulder complaint I have been unable to participate in a joint response from any on the institute's of which I am a member. However, as a qualified Chartered Accountant, a Chartered Insurance Practitioner and an Associate Member of the Institute of Risk Management in the UK, I believe I should contribute as I feel I have something to add.

My apologies for missing the end of July deadline because of my medical problem to endeavour to assist I am e-mailing this to you. I do hope that my comments can still be considered?

**a) The terms Risk Management and Internal Control**

I have never seen any satisfactory explanation of the difference between these terms. The attempts are often both complex and academic, whereas the terms are in practical use every day in many businesses. I believe that it is key to either accept that these terms are in fact one in the same, or, to define risk management as pro-active and both pre and post-event and internal control, at least in operation as post-event, or, to clearly define the differences between the terms in a simple way that will be understandable to users, for instance, by use of a Venn Diagram.

I believe that the Federation is uniquely placed to solicit responses from the key accountancy bodies and those responsible for setting the financial reporting standards, such as the IASB, as well as the leading institutes and associations for insurance and risk management, and academic institutions throughout Europe on this point, and I would urge you to do so!

My point is evidenced yet again, both in your Discussion Paper and within the Revised Turnbull Guidance, which is now in its second consultation period (which concludes on 16 September 2005, and to which they Federation may care to submit an input). Both these documents give definitions of Internal Control in their appendices, but neither offers a definition of risk management. Both documents hedge the issue by referring to the two terms together almost throughout so that the spectrum is fully covered, if in fact it needs to be. I believe this displays the uncertainty that exists about the terms and that it is fundamental that this is to be addressed if the documents are to be creditable.

Why do I think this is so important?

Having spent half my working life, now in excess of 30 years, working either as an external financial auditor or working in industry in senior positions as an accountant/Financial Director, and the other half working in risk management and insurance, I believe that professionals in both these camps perceive a boundary to their areas of influence within their organisations and part of this boundary is set by their perceive roles in the areas of internal control and risk management, which they believe are some how different but no one can quite explain why. The risk manager may therefore often see say, a treasury risk, as something the accountants and auditors should be bothering with. Whilst accountants and auditors believe that some legacy risks and risks associated with self retentions under an insurance programme particularly in structured through a captive insurance company or SPV, as something for the Risk Manager, who will somehow know to bring it to the attention of the accountants if it is material to the financial reporting! Quite how they are expected to know when they are often not given a formal education or training on financial reporting is a mystery.

I do not think that either camp ever really understands the other and as such areas that should be of concern can slip through the net and are not addressed by either. [I now specialise in the area of environmental risk finance and the legacy liability issues in this field are a case in point. Explanations received in regard to 'on balance sheet' property valuations ignoring estimated remediation/clean-up costs for past contamination, and the potential third party liabilities for property damage/bodily injury (illness) caused by the contamination not being considered because of convenient interpretations of IAS 37/FRS 12, are a clear case of an issue which may be fundamental to financial viability of the enterprise not being deemed inside the remit of the accountants who report of the financials or risk manager who is focusing on on-going risk often without consideration to the potential historic liabilities that may have been inherited by their organisations).

Returning to the core argument, by defining the terms internal control and risk management you will facilitate the opportunity for proper governance to be established and ownership of the 'problems' to be defined.

Should it be concluded that there is no difference then either the accountants or the risk manager can be given the overall authority. Indeed, simply by doing this their organisation's governance will be enhanced.

**b) Questions for commentators**

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

   I agree with FEE. The timing is also important as the longer this is left the greater the divergence in approaches that will develop. At this time there is the voluntary disclosure camp (such as the Turnbull/Combined Code approach) and the prescriptive, 'tick the box' disclosure approach (an example of this being the Sarbanes–Oxley Act requirements). The harmonisation on the use of IFRS/IAS provides a window of opportunity to focus on all matters pertaining to financial corporate governance and the Federation needs to maximise this opportunity.

   One word of caution. Better risk management is likely to lead to disclosure of potential liabilities that have not been disclosed previously. This could have material impacts on the profitability and even the perceived financial viability of enterprises. It will thus be key to ensure that there is a realistic phased, realistic and commercially sensitive approach to any

new disclosure requirements. Many bodies will need to contribute to the way forward and this will include government input as lower profitability could impact on the level of their company tax revenues.

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 there is a pressing need to deal with issues relevant to a wider range of entities and stakeholders? If so, please explain.***

I agree with the focus on listed companies as a first stage. However, I believe some research needs to be carried out on who the majority of the shareholders are? The requirements of the man in the street as a shareholder and likely to be very different from the large pension funds investing in the stock market. So it is important to understand who the shareholder is before over-burdening industry with disclosure requirements that the shareholder might not benefit from. Clearly once it is understood who the shareholders are, it would be right and proper to ask them to contribute to the debate, albeit we may have to devise new ways to bring the debate to their attention.

The next stage is to look at other stakeholders and interested parties here I am thinking of banks, government regulators and Inland Revenue/Tax Officials. Their needs from both listed and private companies are likely to be similar. Harmonisation of disclosures to meet their needs may reduce the burden on organisations for voluminous and even multiple reports.

In short, I agree with the initial focus, but feel it is time to address the needs of other users of the Audited Annual Report and Accounts. This may well have impacts on the roles, education, training and development of the directors, particularly Non-Executive Directors, and of the independent external auditor.

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: reasonable liability? If not, please provide details.***

There must be a business case, but it is whom the cost-benefit of the business case is being measured for that is key. Perfect disclosure carries cost burdens to the enterprise that may cause shareholders to divest and move their capital elsewhere it returns are diminished by the cost of compliance. Thus it is important that we firmly establish whom the changes are meant to benefit and secure their buy-in to the cost of the change. Otherwise this will be come an exercise for the academics and not be commercially viable in the business world at large.

Before imposing laws it is key that we understand whether those currently charged with governance are the correct parties? Have they had the necessary academic and on-the-job training and experience? If not where will we be able to draw the nucleus of appropriate people from? I am thinking specifically of the roles that we require directors and officers, and in particular Non-executive directors, to fulfil. We cannot simply make them accountable at the stroke of a pen if they do not have the skills necessary to carry out the role we would envisage for them!

***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.***

It is difficult to comment without clear definitions of the two terms.

I believe that some overriding principles are identifiable and I would commend to you the Risk Management Model produced by the Institute of Risk Management (IRM) in the UK (www.theirm.org). The key to this is its simplicity and hence the ease of understanding for non-risk management personnel. Subject to whatever definitions are adopted for the two key terms I believe that the simple diagrammatic approach has many merits and using the IRM model as a base would in my view be an excellent start.

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

I do not thing the matrix is useful. There is a danger in imposing such standards that a complete the box approach is adopted so that the form becomes more important than the substance.

I do not believe FEE should be so prescriptive, at least at an initial stage, but rather to set the higher framework goals as regards: Identification, Assessment/Evaluation, Control (physical and financial), monitoring, revising/modifying, and reporting, on a continuous cycle. The 'How to achieve this stage' will follow on, if there is buy in to the goals. Giving too much too soon will give rise to unnecessary confusion that will probably evidence itself as rejection.

6. ***Is there a need to develop and 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?***

Once the terms are defined then an EU framework would be beneficial. Once again I would stress my belief that this needs to be set at a high level and not fall into the trap of being overly detailed or complex.

I would again suggest the IRM Risk Management Process is a good guide to the type of framework that is needed at this initial stage.

Once buy-in has been obtained it may then be appropriate to get into further levels of detail.

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?***

I am concerned that enterprises are being asked to produce more and more information and reports and that some simplification needs to emerge. In the UK we see The (audited) Annual Report and Accounts, which includes a Report of the Directors, A Statement on Internal Control/Corporate Governance Statement, and an Operating and Financial Review. In addition many companies produce a Chairman's Report and in a separate document a Social and Corporate Responsibility Report. Despite all this a shareholder does not know if a company has conducted a review of its insurance programme, or indeed whether the company purchases any insurances other than for those few classes of business for which statutory insurance is mandatory. More reports do not necessarily lead to more information being provided. Rather than be concerned with overlap I believe FEE should be advocating a review of what entities are being required to report and why and flowing out from this will be the definition of what risk management aspects need to be, and should be reported on, to whom, in what format and as a standalone document or part of another annual report?

Turning to a specific whilst the bullet point: 'The performance of risk management and internal control should be reported against stated criteria', sounds good I do not know how this can be achieved in practical terms in order to be consistent from one entity to another? Once more I fear FEE is trying to go too far too fast.

As regards specifics I would like to see the following aspects disclosed by entities:

- That the risk finance programme has been review ed by the directors in the course of the year under review and in their opinion the level of self Insurance and risk transfer though insurance and by other means is appropriate for the company/group whose results are being reported on.

  Furthermore, where a group has a captive insurance subsidiary company I would also like to see some specific disclosures in regard to this including some disclosure in regard to the capital adequacy and solvency margin.

- I would like listed companies to disclose the names and addresses of their Insurance Brokers, Risk Management Consultants and any environmental consultancies, whenever external parties are used in order that stakeholders can decide whether these parties are appropriate for the size of the entity reporting. (In the same way as the external auditors, and often the main banks and investment brokers are disclosed).

  When these roles are performed in-house then the qualifications and experience of the key members of staff should be disclosed to the shareholders in the Annual Risk Management/Corporate governance Report.

- I would like to see some brief CVs for all the Non-Executive directors included in the financial statements setting out their qualifications and experience, so shareholders can understand whether they are appropriate people to protect their interests. Much has been said about the need for independent Non-Executive directors in other documents, but I do believe appoints should be for a maximum period and that the Non-Executive directors should be required to retire on a rota basis (saw one-third each year).

These are simple fundamentals that will bring about enhancements to risk management and it is most important that these macro issues are address before going into some of the detail proposed in the paper.

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

Yes.

However, I would suggest that the proposal goes a stage further. Going on to state there should be a requirement that the valuation of all Fixed Assets, both tangible and intangible, to be reviewed of a cyclical basis, say one-fifth by value each year, with all such assets falling for review within a single 5-year cycle. Adequate records should be maintain to support the

existence and ownership of these assets as well as thee current carrying values reflected on the face of the balance sheet, subject to the lower of cost and net realisable value criteria. Included in this should be a requirement for at least desktop environmental surveys to be carried out for all properties owned or leased, and for valuations to be reduced by any estimates for clean-up costs reported on in environmental survey reports which should be compiled by suitably qualified independent specialists.

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?***

I would refer you to the comments made in Section (a) above.

I believe the terms need simple, clear definitions and that FEE is uniquely placed to facilitate dialogue with appropriate bodies to achieve this and to secure then endorsement of the definitions produced. The key is that users in industry understand the terms in the same way as academics and regulators.

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

It is my belief that regulatory requirements should be used only to set high level criteria and to encourage voluntary disclosure.

The regulations need to set a time frame for such voluntary disclosures to be instituted, and at the end of this period the success or otherwise of this approach needs to be assessed. If the voluntary disclosures are not being widely made at that time, initially fines and penalties should be used to motivate compliance, but if this does not bring about the improvement, companies should be advised at the outset that a more prescriptive and mandatory Sarbanes-Oxley type disclose criteria will be introduced to force the disclosures required for compliance.

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?***

It is necessary to define the terms before we can go onto the next stage.

As will be clear from this paper I believe simple aspects such as declarations of insurance programmes, declaration of current off-balance sheet liabilities need to be addressed. It is my belief that GAAP intends for this to be the case but industry is not complying and need to be brought into line.

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

I feel this is attempting to go into the detail when there are fundamentals that should be addressed first before this level of detail can be gone into.

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

No.

I repeat my concern over the lack of evidence of any review of the adequacy or otherwise of the risk finance (including insurance) programme that is in place and whether the company is taking appropriate external advice in regard to this programme.

Currently, two companies could produce what are apparently identical sets of accounts, which present the same facts to stakeholders and potential stakeholders. However, what is not made known is that one of these companies only purchases the minimum statutory insurances whilst the other is extremely risk adverse and purchases as much insurance as it is reasonable able to do with minimum levels of deductible. Hence, one company offers a much higher risk than the other, but this is not clear from the current financial statements or the audit undertaken on them.

I have already set out above proposals that will overcome this issue.

Furthermore, I believe that current audits for on the items included in the accounts the omissions/non-compliances are not adequately probed as evidenced by the financial failures resulting from off-balance liabilities not being taken into account when they should have been. Again I would use the disregard of clean up cost liabilities when valuing property assets to illustrate this.

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

I don't think there are external bodies that can give assurance at this time as neither auditors or regulators have either the training or experience to do so. In addition, the diversity of businesses may make external assurance impossible.

My belief is we should look to the Non-Executive Directors for these assurances and they should "sign off" on a statement on risk management.

To give stakeholders assurance that this sign off is meaningful I believe a regulator should approve who is qualified to act as a Non-Executive Director and the regulator, such as the Financial Services Authority (FSA) in the UK, should maintain a register of approved persons. In addition to maintain some independence the Non-Executive directors should only be permitted to be appointed for a maximum period and should have to retire by rotation.

As previously stated I also believe companies should be required to disclose in their Annual report and Accounts the names and addresses of their key risk management advisers, such as their Insurance Brokers, and any Risk Management Consultants and so forth, so that stakeholders can form an opinion as to whether the company is taking appropriate external advice from appropriate advisers.

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?***

- Establishing clear and simple definitions of the terms Internal Control and Risk Management and getting wide buy in to the definitions.

- Taking a phased approach. If new disclosures are anticipated to adversely impact profitability then this will produce a barrier. There needs to be buy in to what needs to be done, followed by a period of adopting these new rules and then followed by a phase in period in regard to financial impacts that may arise. This will require industry, government, accounting standard setters, revenue/tax authorities and regulators co-ordinating.

- Making some one accountable for disclosures on risk management, including a comment on the risk finance/insurance programme that has been put into place, such as the Non-Executive Directors. (See notes on who should be able to undertake this role and their period of appointment earlier in this paper).

  At this time the external auditors already comment on internal control.

- Advising industry that they will be held accountable and if voluntary disclosure is not fully and properly followed then disclosures will be mandated.

- Getting shareholders and industry engaged in the dialogue by increasing the profile of the dialogue through the institutes and associations (and the membership) to which FEE has contact.

Sincerely,

**Robert J. Martin B.Sc(Hons), FCA, FCII, AIRM**

38A HAUXTON ROAD • CAMBRIDGE • CB2 5HJ, UK
PHONE: +44 (0)1223 847687 • E-MAIL: MARTINRJ29@AOL.COM