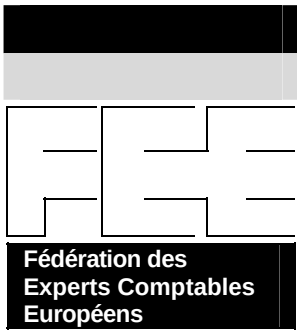

ANALYSIS OF RESPONSES TO FEE DISCUSSION PAPER ON RISK MANAGEMENT AND INTERNAL CONTROL IN THE EU

A COMMENT PAPER

May 2006

FEE

The Fédération des Experts Comptables Européens (FEE) is the representative organisation for the accountancy profession in Europe. FEE's membership consists of 44 professional institutes of accountants from 32 countries. FEE member bodies represent more than 500,000 accountants in Europe.

PURPOSE OF THIS COMMENT PAPER

FEE published a Discussion Paper in March 2005, "Risk Management and Internal Control in the EU", with a view to inviting comment from audit firms, professional accountancy bodies, national auditing standard setters, the International Audit and Assurance Standards Board (IAASB), companies and other interested stakeholders.

FEE has summarised the responses to the Discussion Paper in this paper and commented on these where we thought it necessary to clarify the position. The summary of the responses is presented in this report in order to provide conclusions on each of the questions. The conclusions have been developed based on the comments received, discussions at the FEE Forum on Risk Management and Internal Control of 25 October and further reflections within FEE since the publication of the Discussion Paper. The summary of the responses is condensed and should be read in connection with the individual responses available on the FEE website (www.fee.be). This summary report is expected to be useful to policy makers, standard setters and regulators in the context of obtaining wider experience for the potential development of proposed policies in the area of risk management and internal control. This report should also be a valuable tool for business, investors and the accounting profession, be it at national or international level, when responding to any proposals or new codes, rules, regulations and standards.

It will also be clear that the debate on risk management and internal control remains on the corporate governance agenda for the time being and that practical experience of various approaches continues to evolve. For example:

- Since the issuance of the FEE Discussion Paper in March 2005, the European Union legislative initiatives related to risk management and internal control, including the Statutory Audit Directive and the amendments to the Fourth and Seventh Directives, have been finalised and will need to be implemented by European Union Member States in the near future;

- Some European Union Member States have taken further steps during the last year to amend their laws, regulations, codes or practices in the area of risk management and internal control.

Comments were submitted by[1]:

Professional accounting bodies
- Chartered Institute of Management Accountants (CIMA) (UK)
- Compagnie Nationale des Commissaires aux Comptes (CNCC) – Conseil Supérieur de l'Ordre des Experts-Comptables (CSOEC) (France)
- Foreningen af Statsautoriserede Revisorer (FSR) (Denmark)
- Institut des Réviseurs d'Entreprises (IRE) (Belgium)
- Institute of Chartered Accountants of Scotland (ICAS) (UK)
- International Federation of Accountants (IFAC) - Professional Accountants in Business Committee (PAIB)
- Royal NIVRA (Netherlands)

Auditors
- Auditor General Victoria (Australia)
- Deloitte Touche Tohmatsu
- Ernst & Young
- Grant Thornton (UK)
- KPMG LLP (UK)
- PricewaterhouseCoopers

Companies and their representative organisations
- Confederation of British Industry (CBI) (UK)
- European Association for Listed Companies (EALIC)

Standard Setters and Regulators
- International Federation of Accountants - International Auditing and Assurance Standards Board (IAASB) Steering Committee
- German Accounting Standards Committee (GASC) (Germany)
- Instituto de Contabilidad y Auditoria de Cuentas (ICAC) (Spain)

Risk managers and internal auditors
- Association of Insurance and Risk Managers (AIRMIC) – Institute of Risk Management (IRM) – Federation of European Risk Management Associations (FERMA) (UK)
- European Confederation of Institutes of Internal Auditing (ECIIA)
- Robert J. Martin (Aon Limited) (UK)

No written responses were received from investors and analysts. Policy makers, standard setters and regulators would also have to involve them when developing potential policies in the area of risk management and internal control.

[1] The summary in this report was made by FEE's Working Group on Internal Control, with emphasis on the comments addressing the substantial issues in the discussion paper. Individual respondents may have emphasised other aspects than those mentioned in the summary.

CONTENTS

Purpose of this Comment Paper 4

1. Executive summary 7

2. General comments 8

3. The case for risk management and internal control 10

4. Overriding principles 13

5. Issues to be addressed 15

6. Regulatory options and proposals 19

7. External assurance 25

1. EXECUTIVE SUMMARY

This FEE paper sets out the views of a number of respondents, including audit firms, professional accountancy bodies, companies and their representative organisations, risk management organisations, internal auditors, the IAASB and the International Federation of Accountants Professional Accountants in Business Committee (PAIB), on the issues raised in the FEE Discussion Paper on "Risk Management and Internal Control in the EU" published in March 2005. It provides conclusions based on these comments and further reflections.

The views of FEE were generally consistent with considerations expressed by:

(a) Participants at the event held by FEE in October 2005 to discuss the issue of risk management and internal control; and
(b) The European Corporate Governance Forum in its annual report for 2005. The Forum keeps close track of the developments in the field of risk management and internal control.

Generally, the respondents welcomed the FEE Discussion Paper. However, on a number of FEE proposals, the respondents showed a diversity of views:

- Respondents agreed that it was not desirable to introduce a European equivalent of Section 404 of the Sarbanes-Oxley Act, although Europe should learn from the US experience;
- They also generally agreed that it is not necessary to develop an EU Framework for internal control;
- There is agreement on the idea that a company should keep proper accounting records and that the law should make it mandatory;
- The FEE regulatory principles and the principles of disclosure were broadly supported;
- A majority of respondents are in favour of an evolutionary approach to any further regulation, and support the need for high level criteria to provide meaningful descriptions of internal control and risk management as envisaged by the amendments of the Fourth and Seventh Directives;
- There are divided views on whether it is necessary to focus only on listed companies; and
- Most respondents confirmed their understanding that an audit is designed to express an opinion on financial statements and does not provide specific assurance on internal control. There were divided views on other assurance issues.

It should be noted that participants at the FEE event included a broader range of backgrounds and experience than respondents to the FEE Discussion Paper. Participants included individuals from the business and investor communities from a number of European Union Member States, as well as the auditing profession. Membership of the European Corporate Governance Forum is similarly broadly based.

2. GENERAL COMMENTS

All respondents were broadly in favour of the views set out in the FEE Discussion Paper on Risk Management and Internal Control in the EU and they offered a lot of valuable, positive comments. A limited range of respondents volunteered different views as discussed in further detail in the detailed responses to the questions.

The main views are identified in the Executive Summary. Looking to the future, it is suggested that:

- The debate on risk management and internal control needs to remain open for the time being, particularly in view of the differences between the US and the European approaches;
- Practical experience of various approaches on risk management and internal control continues to evolve resulting in a need to review how these approaches work in practice; and
- There is a need to consider the scope for greater convergence.

In this respect, it is also significant to refer to the discussions at the FEE Forum on Risk Management and Internal Control in the EU of 25 October 2005[2]. This event attracted over a hundred participants representing a wide range of stakeholders from regulatory, business, investor and auditing spheres.

The discussions at the FEE Forum emphasised the following ideas:

- The European Commission will not follow a prescriptive approach, which is welcomed;
- A broad-based approach to internal control which does not focus solely on financial reporting controls is widely supported;
- It is right to carry out a cost/benefit analysis and to take care about unintended consequences of prescriptive regulations;
- There is no evidence of demand for public reports on effectiveness of internal control in Europe;
- Investors were more interested in descriptive material about risk management, which would allow the market to take the lead in developing risk management;
- The US authorities have the possibility to revisit PCAOB Auditing Standard No. 2 and to amend the prescriptive approach within the existing legal framework;
- Legislation on risk management must not cause managers to refrain from accepting risks;
- Further regulation and disclosure will also not stop people who lack integrity from committing crimes;
- Implementing the proposed amendments to the Fourth and Seventh Directives is a national issue but it will be important to look at what solutions will be selected by Member States. Some of them already have very demanding systems (for instance in the Netherlands), others have no requirements as yet. The area of internal control and risk management is fertile ground for convergence within Europe;
- Learning from practical experience of various approaches in risk management and internal control should continue; and
- Financial scandals have previously encouraged regulatory actions. This emphasises the importance of debate and understanding ahead of any potential future scandal. Therefore, the debate on risk management and internal control remains on the agenda.

[2] http://www.fee.be/news/default.asp?library_ref=2&content_ref=518

It is also worth indicating that the European Corporate Governance Forum which comprises individuals from a broad range of relevant stakeholders across Member States, established by the European Commission decision of 15 October 2004, commented on the FEE event in their Annual Report 2005[3] as follows:

"The Forum also discussed the outcome of the event conference on Risk Management and Internal Control that was organised on 25 October 2005 in Brussels by the European Federation of Accountants (FEE) following its consultation launched in March 2005. The views expressed at the conference supported the Forum's own conclusions. Thus, participants shared the Forum's concerns about the costs of the US approach to internal control and also at the conference no calls were made for the introduction of an effectiveness statement or of public reporting of auditors. However, just as the Forum also the conference participants felt that the work in the field should go on in order to keep close track of the developments."

[3] http://www.europa.eu.int/comm/internal_market/company/docs/ecgforum/ecgf-annual-report-2005_en.pdf

3. THE CASE FOR RISK MANAGEMENT AND INTERNAL CONTROL

Question 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.

FEE Discussion Paper

Improvements in business risk management and related disclosure have not been and should not be driven by regulatory requirements alone. The introduction of regulatory requirements should be based on proper evidence about the likely costs and benefits.

Many EU Member States have taken initiatives and have introduced requirements on risk management and internal control. However, there is a risk that such national initiatives will work against the integration of capital markets within Europe. Therefore, FEE supports discussion of risk management and internal control at the European Corporate Governance Forum and believes it is desirable that work is done on a European level to develop common overriding principles.

Summary of the Responses to Question 1[4]

The vast majority of the respondents are of the opinion that there is a need to promote discussion and evidence gathering related to the many different initiatives taken by EU Member States on risk management and internal control. As the systems put in place in different EU Member States vary considerably, there is a need for a sound and common understanding of the current situation in the EU.

This does not mean that there is widespread support for a harmonised system of risk management and internal control in the EU, and for further regulation driven by the European Union. Rather what is important is the dissemination of market based best practice and learning from experience.

FEE Conclusion

There is strong support for further discussion, evidence gathering and learning from experience in the development of risk management and internal control.

[4] The summary in this report was made by FEE's Working Group on Internal Control, with emphasis on the comments addressing the substantial issues in the discussion paper. Individual respondents may have emphasised other aspects than those mentioned in the summary.

Question 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.

FEE Discussion Paper

Risk management and internal control are vital to the governance of any organisation. However, there is a presumption that some regulatory requirements in relation to risk management and internal control would need to apply to all listed companies because they necessarily expose the public to the residual risks borne by equity shareholders.

Summary of the Responses to Question 2

Respondents agreed that public policy on risk management and internal control in the EU should in the first place focus on listed entities and the needs of their shareholders. Listed entities should set the tone. This is evidenced by the following quotation:

"The focus on listed entities and the need of their shareholders is appropriate.[5]"

At the same time respondents recognised that risk management and internal control are relevant for all companies. Although the focus should be on listed entities, public policy on risk management and internal control should be expanded to public interest entities[6] where there are equal public expectations.

Risk management and internal control are also important in all other companies, but this raises questions on the 'degree' of applicability. For instance, the management of risks including their identification and evaluation, responding to them and concluding internally on the effectiveness of their management as well as disclosure of the overall process of risk management and disclosure of management of specific risks internally within the company should be best practice in every company.

However, public disclosure of such information is primarily supported for listed entities and also, to some degree, for public interest entities. It is acknowledged that the inclusion of public interest entities in public policy on risk management and internal control will require the introduction of exemptions, for example for small public interest entities.

Few respondents commented on the needs of other stakeholders, which was considered as a sort of "next step" only.

5 Ernst & Young

6 As defined in the Statutory Audit Directive which was approved by the European Parliament on 28 September 2005 and by ECOFIN on 11 October 2005.

FEE Conclusion

While public policy on risk management and internal control should in the first place focus on listed entities, aspects of it are also relevant to other public interest entities and all other companies.

4. OVERRIDING PRINCIPLES

Question 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.

Question 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.

FEE Discussion Paper

Overriding principles

- *The business case for risk management: Risk management and internal control requirements should seek to reflect sound business practice, remain relevant over time in the continually evolving business environment and enable each company to respond to the specific needs of the business of the company.*

- *Advantages of principles-based requirements: Recognition that risk management and internal control need to be responsive to the nature and needs of the business also means that any requirements should be framed in terms of the high-level objectives or principles to be achieved. Agreement on principles is also important in a EU context because it allows for national variations whilst building confidence across a single market.*

- *Distinctive features of listed companies: Risk management and internal control are vital to the governance of any organisation. However, there is a presumption that some regulatory requirements in relation to risk management and internal control would need to apply to all listed companies because they necessarily expose the public to the residual risks borne by equity shareholders.*

- *Primacy of those charged with governance: Risk management and internal control are the responsibility of those charged with governance in the company and should be embedded in the business and the actions of its management and employees including the internal audit function.*

- *Reasonable liability: Carrying on a business necessarily involves taking risks and returns reflect rewards for taking risks. Any regulatory requirements need to recognise that there are balances to be struck in terms of the degree to which the risks faced by investors can be managed and the extent of the liability borne by those charged with governance and other parties. Liability should be appropriately aligned to the level of responsibility taken and should encourage the use of reasonable judgment, useful disclosure and fair enforcement.*

Summary of the Responses to Questions 3 and 4

Most of the respondents agree that the case for introducing any regulation related to risk management and internal control should have regard to the overriding principles set out by FEE. There is however a minority view that it is necessary to provide detailed guidance on how to implement principles. Additionally, few respondents are convinced that there is actually a need for regulation relation to risk management and internal control.

As far as the identification of additional overriding principles relevant to risk management and internal control is concerned, some respondents raise some practical issues in relation to the implementation of some of the principles:

- Because of their flexibility, overriding principles will vary depending on the country and will need to be adapted to the environment of the country, the industry or sector and the company in which they are applied;

- The introduction and implementation of regulation related to risk management and internal control is not straightforward and requires a significant cultural change within companies;

- Companies should take and manage risk within their risk appetite. The setting of the risk appetite and its regular review should be a key responsibility of those charged with governance;

- The role of stakeholders other than shareholders is also an item that may deserve attention to capture the wider aspects of accountability.

FEE Conclusion

There is broad agreement on the need for overriding principles as proposed by FEE in case a regulation related to risk management and internal control is introduced. Some practical issues in relation to the implementation of FEE's proposed principles were volunteered as well.

5. ISSUES TO BE ADDRESSED

Question 5

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

FEE Discussion Paper

FEE proposed the following matrix to analyse and explain the different issues with respect to risk management and internal control.

Figure 1: Matrix for analysis with respect to companies

			Types of risk		
			Financial reporting	Compliance	Operational and strategic
Types of activity	Manage risks	Identify and evaluate			
		Respond			
		Conclude on effectiveness			
	Disclose	Overall process			
		Management of specific risks			
		Effectiveness conclusion			

Summary of the Responses to Question 5

Respondents were divided in their responses to this question. Some respondents were of the view that the matrix for analysis is clear and useful. Other respondents thought that the matrix was not self explanatory and ought to be expanded or changed. They saw it as moving away from a principles-based approach into a tick-box approach which excludes the use of frameworks other than COSO. It was also suggested by some respondents that the matrix should be aligned to COSO Enterprise Risk Management (ERM). These comments indicate the need to use the matrix with care.

FEE would like to re-emphasise that the matrix was introduced as a tool to systematically analyse and explain the different issues with respect to risk management and internal control. The matrix was not proposed with the intention to set a framework for companies to manage their risks or to apply to internal control procedures. It was instead designed as a way to structure the analysis of risk management and internal control developments across Europe with the aim to suggest European policy responses on the subject.

As indicated earlier, FEE is very supportive of a principles-based approach for risk management and internal control and therefore encourages the use of a wide range of frameworks in this area.

FEE Conclusion

The matrix remains a useful tool for analysis of developments in regulatory requirements and consideration of policy issues, provided it is accompanied by clear explanation as to its purpose.

Question 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?

FEE Discussion Paper

FEE has the following concerns with regards to developing an EU framework for risk management and internal control:

- *The resources required to develop and maintain a framework which satisfies appropriate criteria are substantial;*
- *It is not clear what benefits a new framework would add to the existing frameworks developed by COSO, Turnbull and CoCo; and*
- *In general, FEE is committed to global rather than European solutions.*

Summary of the Responses to Question 6

The majority view of the respondents is best summarised as quoted as follows by one of the respondents:

"We do not believe that there is a need to develop an EU framework for risk management and control. There are existing frameworks, such as the Turnbull Guidance issued by the UK's Financial Reporting Council and the guidance issued by COSO, which could be referred to as "acceptable for the purposes of the Regulation".[7]"

A minority of respondents were in favour of the development of an EU framework.

FEE Conclusion

The majority of the respondents are in favour of high-level principles set at an EU level but not of an EU framework for risk management and internal control.

Question 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?

FEE Discussion Paper

FEE supports the following disclosure principles for risk management and internal control based on the qualitative characteristics of useful information:

- *Disclosure should be useful to shareholders and the benefits derived from the disclosed information should exceed the cost of providing it;*
- *The disclosure should be understandable to an informed intelligent person and not only meaningful to professional investors or those inside the company;*
- *The disclosure of risk management and control information should avoid overlap with information in the financial statements and other disclosures and should make clear the implications of issues identified including the impact on the financial statements of the entity, if any;*
- *The performance of risk management and internal control should be reported against stated criteria;*
- *There should be consistency of reporting between years, to promote continuous improvement of the performance of risk management and control and disclosure of measures taken by the entity to address issues or problems that have arisen, if any; and*
- *Disclosures should link risks to the entity's general business strategy.*

[7] Grant Thornton (UK)

Summary of the Responses to Question 7

Most respondents agree with the disclosure principles for risk management and internal control as proposed by FEE. However, some additional sensitivities should be acknowledged which may be summarised by the following quotations from respondents:

"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]."

"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. The issue of commercial sensitivity may need to be addressed within these principles[9]."

Although not proposed by FEE, a number of respondents have volunteered their views on the public disclosure of effectiveness conclusions on risk management and internal control. They were not in favour of such public disclosure as the following quotation illustrates:

"With regard to a conclusion of effectiveness, this may be useful internally but should not be a matter for public disclosure. While the Sarbanes-Oxley Act has such a requirement, the recent consultation carried out by the Turnbull Review Group in the UK showed that companies and investors ~~there~~ did not consider effectiveness statements to be a useful tool[10]."

FEE Conclusion

Most of the respondents agree with the disclosure principles for risk management and internal control as proposed by FEE. There is no support for public disclosure of effectiveness conclusions. Although public disclosure of company-specific risks is worth considering, respondents acknowledged there are serious concerns about issues of commercial sensitivity.

8 Association of Insurance and Risk Managers (AIRMIC) – Institute of Risk Management (IRM) – Federation of European Risk Management Associations (FERMA) (UK)

9 KPMG LLP (UK)

10 Confederation of British Industry (CBI) (UK)

6. REGULATORY OPTIONS AND PROPOSALS

Question 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?

FEE Discussion Paper

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. Whilst this would not represent a requirement related to risk management and internal control over financial reporting, it would provide a proper foundation for shareholder confidence in financial reporting.

Summary of the Responses to Question 8

All respondents agreed with the FEE proposal that there should be a basic EU requirement for all companies to maintain accounting records that support the information for published financial statements, as such a requirements already exists in a considerable number of EU Member States.

Some were of the view that there are certain practical concerns to implementing such requirements which could be left to the EU Member States to deal with. Some respondents stated that such a requirement could be included in the Fourth and Seventh Company Law Directives which, although currently including requirements related to year-end annual accounts only, could indirectly link into maintaining continuous accounting records that support information included in published financial statements.

FEE Conclusion

There was general support for the FEE proposal.

Question 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?

FEE Discussion Paper

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. These might, for example, clarify whether those charged with governance of the company should disclose the process by which they assess the effectiveness of risk management and internal control.

Summary of the Responses to Question 9

The majority of the respondents favoured developing high-level criteria. However, there is little support for detailed guidance for descriptions of internal control and risk management, both at EU and EU Member State level.

The recognition of the need for some high-level criteria for describing internal control and risk management is often caused by practical considerations. Such high-level criteria can help to acknowledge and reinforce the basic responsibilities in respect of the description of internal control and risk management.

In order to achieve high quality descriptions of the main features of existing internal control and risk management systems in relation to the financial reporting process, it might be helpful to have some principles or criteria to guide companies in formulating their own criteria for describing their systems.

If principles or criteria are established, the following quotation provides examples of criteria that could be set at the highest level:

- "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; and
- An acknowledgement that no system of internal control can provide absolute assurance against material misstatement or loss[11]."

FEE Conclusion

The majority of the respondents support high-level criteria for the description of internal control and risk management. There is little support for detailed guidance in this respect.

[11] KPMG LLP (UK)

Question 10

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

FEE Discussion Paper

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. In proposing an evolutionary path for listed companies to follow over a number of years, FEE is not presuming that there would be any relentless increase in legal requirements at the European level.

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.*

It should also be noted that such mechanisms will be viable in regimes where shareholders have effective power through company law to bring about change and influence those charged with governance. Company law in Europe generally already gives shareholders powers to act.

Summary of the Responses to Question 10

Respondents expressed little support for regulatory requirements in promoting improvement in risk management and internal control and would prefer markets to do this. As proposed by FEE, in case some regulatory requirements are introduced, they should be phased-in gradually over time. Also, there is a clear preference for a "comply or explain" approach to regulatory requirements which allows for required "comply or explain" reporting against corporate governance codes.

FEE Conclusion

There is little support for regulatory requirements to promote improvement in risk management and internal control.

Question 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?

Question 12

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

FEE Discussion Paper

FEE identifies a number of issues for consideration by listed companies and regulators using the matrix of analysis first introduced in Figure 1 in Section 4.1. (See question 5)

1. Issues related to managing risks

It should be recognised that it might be inefficient and ineffective to try to superimpose risk management and internal control on top of existing business practices and that it might be preferable to 'embed' them in business processes and behaviour. This means that major organisational change will often be required before a company will be able to support a statement that it manages its financial reporting, compliance, operational and strategic risks.

2. Issues related to disclosures of overall process

Additional issues that arise related to disclosures of overall process include the following:

- *The apparent desirability of developing high level criteria for the contents of disclosures to enhance usefulness;*
- *The need for clarity about whether disclosures relate to the process as designed or as operating in practice; and*
- *How to avoid lengthy disclosures which change little from year to year; and*
- *The potential commercial sensitivity of disclosures related to operational and strategic risks in particular.*

3. Issues related to disclosures of management of specific risks

The extension of disclosures related to the management of specific risks is subject to major concern about commercial sensitivity and potential liability and reputational damage for directors. In practical terms it can also be very difficult to communicate meaningfully a company's risk tolerances and various risk responses.

4. Issues related to disclosure of effectiveness conclusions

Implementation of Section 404 of the Sarbanes-Oxley Act illustrates the problems that arise when effectiveness conclusions are required to be reported publicly, even in the relatively narrow area of internal control over financial reporting.

A requirement to publish 'black or white' conclusions raises major potential liability and reputational issues for directors and appears to lead inexorably to detailed criteria and rules which set out what is required by way of support for a 'clean' conclusion on effectiveness. In the absence of such detailed rules, it is likely that statements will be subject to such caveats and carve-outs as to severely reduce their usefulness.

Summary of the Responses to Question 11

Most respondents agreed with FEE's identification of the issues for consideration by listed companies and regulators as specified above. Dissenting views focused on the incompatibility of the FEE matrix with the COSO Framework or they disagreed with the acknowledgement by FEE that statements of effectiveness provide a strong incentive to make better disclosures of overall process and the management of specific risks.

One respondent can be quoted to reinforce the majority view against public disclosure of effectiveness conclusions:

"In general a conclusion on the effectiveness can be appropriate, because it allows for ex-post examinations of the management's insight. But a corresponding requirement seems rather difficult to implement at this point in time, also because solid theoretical procedures of measurements of certain risks (besides financial risks) have not yet been established. In the absence of the possibility to measure risk it does not seem reasonable to include requirements to evaluate the risk measurement. Therefore we agree with FEE that it might not be useful to introduce across the EU effectiveness conclusions on internal control over financial reporting as required by Section 404 of the Sarbanes-Oxley Act[12]."

FEE Conclusion

The majority of the respondents agreed with FEE's identification of the issues for consideration by listed companies and regulators as stated above.

Summary of the Responses to Question 12

The following views were offered by respondents:

"We agree that on issues related to managing risks any new requirements should have sufficient lead time to allow them to be embedded into the business, and that disclosures in earlier years may properly be limited to a description of the steps being taken to do so.[13]"

[12] German Accounting Standards Committee (GASC) (Germany)
[13] Deloitte Touche Tohmatsu

"We would like to underscore the FEE comments on issues related to disclosures of management of specific risks, 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.[14]"

"Issues related to disclosure of effectiveness conclusions indicated that on the face of it there seems merit in effectiveness disclosure. Unfortunately, the task of meaningful disclosure does present significant challenges. The step-by-step, evolutionary approach suggested in the paper makes sense. In addition it is important that the views of stakeholders are obtained as to whether they see value in disclosing effectiveness conclusion and, if so, what type of information would prove useful.[15]"

"We had the opportunity to see the evidence published by the Turnbull Review Group (TRG) in the UK. CIMA notes that the TRG has decided that it would not be appropriate to make a report on the effectiveness of the internal control system, but instead, is proposing that boards should be required to confirm that necessary action has been taken or is being taken to remedy any significant failings or weaknesses identified from the review of the effectiveness of the internal control system. CIMA is currently in the process or re-considering its views on effectiveness in the light of the TRG's conclusions, but at this stage, it would be fair to say that our reaction to the TRG's proposals as a whole is one of support for the measured, principles-based approach which builds upon the success of the existing Turnbull guidance. Perhaps, our main conclusion at present is that the effectiveness debate needs to remain open for the time being, particularly in view of the differences between the US and the European approaches, the need to review how SOX works in practice and the need to consider the scope for greater convergence.[16]"

FEE Conclusion

Although most respondents agreed with the issues identified by FEE, they noted a number of other factors which are worth considering when developing regulatory requirements and their practical implementation in the area of risk management and internal control for listed companies, including that the debate remains open for the time being.

[14] European Confederation of Institutes of Internal Auditing (ECIIA)
[15] Professional Accountants in Business Committee (PAIB) of IFAC
[16] Chartered Institute of Management Accountants (CIMA) (UK)

7. EXTERNAL ASSURANCE

Question 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.

FEE Discussion Paper

Currently, the external auditor generally performs work on internal controls in order to be able to issue an opinion on the financial statements of a company. In December 2004, IAASB issued its new ISA 700 (Revised), The Independent Auditor's Report on a Complete Set of General Purpose Financial Statements. This requires the auditor's report to state that "the procedures selected depend on the auditor's judgement, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control". A financial statement audit opinion therefore does not provide any assurance either on disclosures of risk management and internal control not given in financial statements or on the effectiveness of risk management and internal control.

Summary of the Responses to Question 13

Most respondents who answered this question were audit firms and professional accountancy bodies who answered negatively. An audit (for instance under International Standard on Auditing (ISAs)) is designed to express an opinion on the annual financial statements, rather than on the system of internal control. Although the audit report makes reference to the procedures performed on internal control relevant to the company's preparation and fair presentation of the financial statements, this does not specifically provide assurance on the internal control systems, notwithstanding national particularities on the audit scope, e.g. the audit of the risk early recognition system in Germany. Consequently, an audit opinion does not provide for assurance on internal control, although some respondents stated that this is very often misunderstood by a wide range of stakeholders, including directors of companies and investors, which leads to an expectation gap.

One audit firm included in their quotation the following:

"The audit of financial statements is not designed to provide specific assurance on internal controls. 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.[17]"

[17] PricewaterhouseCoopers

A number of respondents also pointed out that there is no difference between substantive "audit" procedures performed by management or by external auditors in respect of internal control systems and their effectiveness.

Some respondents also commented on the existing communication issues and differences. There is some communication by external auditors to those charged with governance and management of the company, which results in some degree of "assurance" to them on internal control systems, but there is no such communication to investors. This communication issue results in the expectation gap as noted above.

FEE Conclusion

Most respondents confirmed that currently an audit is designed to express an opinion on the financial statements and is not directed at providing separate assurance on internal control over financial reporting, notwithstanding national particularities on the audit scope.

Question 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?

Question 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?

FEE Discussion Paper

- *External auditors' provision of assurance services in respect of risk management and internal control cannot exceed the responsibilities assumed by those charged with governance.*
- *Auditors should initially work with those charged with governance to identify useful forms of private assurance reporting on risk management and internal control.*
- *In line with 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.*
- *Further work should be done by the auditing profession to consider how to apply International Standard on Assurance Engagements 3000 (Revised) Assurance Engagement other than Audits or Reviews of Historical Financial Information (ISAE 3000) to provide external assurance on internal control reporting separate from the financial statement audit.*
- *It is essential that auditors' liability fairly and reasonably relates to the consequences of unsatisfactory audit and assurance performance.*

Summary of the Responses to Question 14

Respondents did not give positive answers to this question and some advocated strongly against the integrated audit approach. A number of respondents pointed out that if Europe would go in the direction of the Sarbanes-Oxley Act, Section 404, which no respondent would support, then an integrated audit would be inevitable.

Other respondents did not support the integrated audit approach, as clarified in the following quotation:

"We believe that the development of assurance on disclosures related to risk management and internal control should mirror the implementation of such disclosures, and that there is merit in encouraging companies to voluntarily request limited assurance on entity-wide internal control, without mandating assurance or forcing it to be as detailed as that envisaged by PCAOB Auditing Standard 2[18]."

Some respondents were of the opinion that assurance should not be provided by external auditors but provided by the company's non-executive directors:

"I do not 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[19]."

FEE Conclusion

Respondents were not supportive of the integrated audit concept.

Summary of the Responses to Question 15

Respondents made a variety of suggestions as far as the principal priorities in the possible development of a new form of assurance related to risk management and internal control are concerned.

One respondent was of the view that in view of the huge amount of new rules and regulations which were imposed on companies over the last few years "a period of calm" is now required.

Some respondents were of the view that the likely costs and benefits of assurance should be considered. Other respondents strongly supported the further development of ISAE 3000 to provide external assurance on internal control reporting separate from the financial statement audit.

[18] Deloitte Touche Tohmatsu
[19] Aon Limited (UK)

FEE Conclusion

Respondents proposed a variety of priorities and mentioned the need for a pause in regulation, appropriate analysis of costs and benefits of assurance on risk management and internal control and strong support for further development of approaches based on ISAE 3000.