Risk Management and Internal Control in the EU Discussion Paper

March 2005

CONTENTS

Appendices

1. EXECUTIVE SUMMARY

1.1. Scope and purpose

This discussion paper sets out the views of the Fédération des Experts Comptables Européens (FEE) - the representative body of the European accounting profession – on:

- The case for listed companies in Europe to exercise risk management and internal control in the interests of shareholders; and
- How regulators in the EU and its Member States might encourage improvements in risk management and internal control, without imposing disproportionate regulatory burdens.

FEE does not make presumptions about a need for increased regulation. Good risk management and internal control make business sense and businesses should not be subjected to regulatory intervention without good cause and a proper consideration of the costs and benefits. Moreover, if regulation is necessary, then disclosure of information should be the preferred regulatory tool because it puts power in the hands of shareholders and markets rather than leaving it entirely with regulators.

Although it is envisaged that the discussion paper will primarily be of importance to listed companies, the paper approaches risk management and internal control in a way that is relevant to a wider range of public interest and other organisations. It does this by seeing risk management and internal control from a corporate governance point of view as part of the accountability of a company's board and management to stakeholders. In the context of a listed company it focuses on accountability to the company's shareholders rather than the requirements issued and enforced by a securities market regulator.

The paper responds to a commitment made in FEE's July 2003 Discussion Paper on corporate governance that "FEE is at present undertaking a new project on internal control with an aim to develop a position on how management and those charged with governance and external auditors can responsibly report on companies' systems of internal control in ways that serve the public interest." In FEE's view, there is a need to promote discussion involving investors, business and regulators to inform the development of thinking within the EU on risk management and internal control.

This discussion paper is aimed at those charged with the governance of listed companies, as well as their shareholders, managements and auditors, and related representative bodies, regulators and legislators. The paper's proposals have been shared informally with a wide range of EU stakeholders and bring together four main pieces of work:

- An understanding of current best practice amongst companies in risk management and internal control;
- A review of recent regulatory developments in response to financial scandals in the United States and Europe;
- Recent European Commission thinking and related proposals on corporate governance; and
- A survey of regulatory requirements on risk management and internal control in certain EU Member States applicable outside regulated financial services.

In financial services industries, there are generally wide-ranging requirements in relation to systems and controls which are the subject of internal reporting arrangements involving financial institutions, regulators and external auditors. This paper is not concerned with such industry-specific requirements

nor does it address public sector entities. Nevertheless, issues and proposals discussed in this paper may be of wider relevance to these sectors.

In addition, whilst it is recognised that serving the long-term interests of shareholders involves having regard to the interests of other stakeholders, this paper does not specifically address the risk management needs of such stakeholders.

Recent financial scandals in the United States and Europe demonstrate the need for those charged with governance of listed companies to manage risk effectively and to be seen to do so if they are to reinforce confidence in capital markets and create sustainable value. The aim is over time to establish securities markets in Europe where all listed companies are expected to:

- Manage their risks actively;
- Assess how effective they are in doing so; and
- Make appropriate related disclosures to shareholders.

The paper sets out various proposals as to how European regulators can build on what the best companies are already doing. However, the introduction of any requirements should be based on evidence that the likely benefits to companies and their shareholders will exceed the costs involved.

1.2. Some observations on the US Sarbanes-Oxley Act

The Sarbanes-Oxley Act should be viewed in the context of the US legislative framework and the limited rights of shareholders in the United States. Company law in Europe generally gives shareholders powers to act which are not generally available to US shareholders under US state corporation law, and the further strengthening of shareholders' rights is high on the European Commission's agenda.

European shareholders do not therefore necessarily need to look to a European equivalent of US federal securities legislation, such as the Sarbanes-Oxley Act, to bring about improvements in risk management and internal control. There are already viable mechanisms in Member States where shareholders have effective power through company law to bring about change and influence those charged with governance.

This discussion paper nevertheless outlines the relevant requirements of two sections of the Sarbanes-Oxley Act which deal with different types of internal control. Section 404 which covers internal control over financial reporting, and the less high profile Section 302 which covers disclosure controls for information in reports that are filed with the Securities and Exchange Commission (SEC).

Section 302 and its related SEC rules contain a number of requirements related to SEC-required disclosures. Two senior executives of the company are required to maintain, and regularly report publicly on their evaluation of, disclosure controls and procedures that ensure that the information required to be included in reports filed under the Securities and Exchange Act (1934) is recorded, processed, summarised and reported on a timely basis. These two senior executives, primarily the CEO and the CFO, are required to certify the information contained in the quarterly (for US domestic registrants of the SEC) and annual reports. The officers also make further certifications about controls over reporting processes. In particular, they are required to certify that they are responsible for establishing, maintaining and regularly evaluating the effectiveness of the company's disclosure controls and procedures; have made certain disclosures about internal controls to the company's audit committee and its auditors; and have included information in the quarterly and annual reports filed with the SEC about their evaluation.

Section 404 and its related SEC rules cover financial reporting controls and require management to publicly state their responsibility for establishing and maintaining adequate controls over financial reporting together with an assessment of their effectiveness at the end of the most recent fiscal year. External auditors, as required by Auditing Standard Number 2 issued by the US Public Company Accounting Oversight Board (PCAOB), must perform detailed work that will enable them to provide three audit opinions on:

- The financial statements of the company;
- Management's assessment of the company's internal control over financial reporting; and;
- The auditor's own opinion on the company's internal control over financial reporting.

FEE is supportive of the objectives of board accountability for the preparation of information to shareholders and that companies should establish and maintain effective systems of risk management and internal control to safeguard shareholders' investment.

FEE also recognises that there are substantial differences between the methods for realising such objectives in the United States within its legislative and regulatory framework and the way that these principles can be achieved via a European framework of company law and codes of corporate governance, including shareholder rights which enable shareholders to bring about change.

FEE is currently not convinced about the idea of introducing across the EU an equivalent requirement to Section 404 of the Sarbanes-Oxley Act as to whether or not internal control over financial reporting is effective. Nevertheless, FEE is keen to understand the views of commentators, to learn from experience of implementing Section 404 and from consultations with company and investor groups carried out across EU Member States. Experience of implementing Section 404 should include an assessment of whether the benefits to shareholders exceed the costs of complying with all the requirements related to Section 404. This assessment should then be viewed in the context of the existing requirements of company law and corporate governance frameworks in the EU and its Member States.

1.3. Key proposals

- Emphasis should be placed on an overall need for more research and learning from experience to direct developments in risk management and internal control appropriately. It also needs to be widely recognised that profits are, in large part, the reward for successful risk-taking. Therefore the purpose of risk management and internal control is to manage risk, including upside risk, appropriately rather than to eliminate it. (Sections 2.3 and 3.1)

- There is a need for principles to underpin any regulatory developments in risk management and internal control. (Section 2.3)

- It would be appropriate to reflect existing Member State requirements by introducing a basic EU requirement for all companies to maintain accounting records that support information included in published financial statements. (Section 5.4)

- Phasing of the introduction of the proposed internal control-related requirements in the Eighth and the Fourth and Seventh Directives would be sensible to recognise that some companies and some Member States may face implementation challenges that will take time to resolve. (Section 5.4)

- 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 (Section 5.4)

- 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. (Section 5.5)

- 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. (Section 5.5)

- FEE is currently not convinced about the usefulness of introducing across the EU published effectiveness conclusions on internal control over financial reporting as required by Section 404 of the Sarbanes-Oxley Act. However, it will be important to take account of the views of investors and companies and forthcoming evidence about the usefulness, costs and benefits of such conclusions to investors as Section 404 of the Sarbanes-Oxley Act is implemented. (Section 5.5)

- External auditors' provision of assurance services in respect of risk management and internal control cannot exceed the responsibilities assumed by those charged with governance. (Section 6.1)

- Auditors should initially work with those charged with governance to identify useful forms of private assurance reporting on risk management and internal control (Section 6.6)

- 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. (Section 6.6)

- Further work should be done by the auditing profession to consider how to apply ISAE 3000 to provide external assurance on internal control reporting separate from the financial statement audit. (Section 6.6)

- It is essential that auditors' liability fairly and reasonably relates to the consequences of unsatisfactory audit and assurance performance. (Section 6.6)

2. THE CASE FOR RISK MANAGEMENT AND INTERNAL CONTROL

2.1. Best practice for companies

In the wake of major financial scandals in the United States and Europe, public confidence in capital markets and listed companies has been damaged. Companies need to address these concerns and reinforce public trust in capital markets by acting responsibly, creating value for their shareholders and being seen to do so.

Those charged with governance of a company are expected to act in the interests of shareholders and identify, evaluate and respond to the company's risks. These risks encompass risks related to strategy and business operations as well as risks related to compliance with laws and regulations and financial reporting. Shareholders expect those charged with governance of the company to inform them about the risks the company they invested in is facing and also to put controls in place to deal with such risks.

There are a number of definitions of internal control in various guidance documents such as the COSO (USA), Turnbull (UK) and CoCo (Canada) frameworks. Whilst there are some differences in these definitions essentially, internal control is a "process" established, operated and monitored by those charged with governance and management of a company to provide reasonable assurance regarding the achievement of the company's objectives. "Process" is used in a broad sense; it goes beyond procedures and also includes elements such as corporate culture, systems, structure, policies and tasks. It is upon this process approach that much of the guidance in EU countries on internal control is now concentrated.

A definition of risk management is identified in the COSO Enterprise Risk Management (ERM) – Integrated Framework as follows: Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. However, there are other definitions of risk management and consequently this definition is not uncontroversial.

COSO ERM – Integrated Framework defines internal control as a subset of risk management as risk management is concerned with the wider external and internal risks relevant to the determination of the entity's strategy to reach the entity's objectives whereby internal control structures and procedures are instrumental in achieving these objectives.

A key point here is that those charged with governance should adopt a risk-based approach to internal control and any assessment of its effectiveness. This means that internal control is relevant to the broader subject of risk management because it serves to mitigate the gross or inherent risk involved in a business activity and determine the net risk borne by a company. This approach should be incorporated into the strategic, governance and management processes of the company and should encompass the wider aspects of internal control, not just those directly related to financial reporting.

In recent years, business risk management and related disclosure to investors have become best practice for companies and are supported by well-established frameworks such as COSO, Turnbull and CoCo. Internal and external auditors are also involved by those charged with governance as they seek counsel as to how risk management and disclosure are to be applied appropriately.

2.2. FEE's support for best practice

Introduction of a risk-based approach to internal control and the assessment of its effectiveness by the people within the business is a major challenge for management and those charged with governance. It takes time, effort and costs and requires cultural and behavioural changes. FEE believes that the benefits of doing so make the effort worthwhile.

In July 2003, FEE stated in its *Discussion Paper on the Financial Reporting and Auditing Aspects of Corporate Governance* that "Systems of internal control and risk management are fundamental to the successful operation of any company, not only for financial reporting purposes but also for the day-to-day running of the company to help it achieve its business objectives."

The Discussion Paper continues: "As the risks facing a company are continually changing, the board should ensure a thorough and regular evaluation of the nature and extent of the risks to which the company is exposed and the controls to manage them. Since profits are, in part, the reward for successful risk taking in business, the purpose of internal control is to help manage and control risk appropriately rather than to eliminate it. It is important to embed risk management into a business. The board of a company, its management and the company's internal audit function are concerned with the management of all the significant risks facing a company, some of which may be directly related to financial reporting."

2.3. From best practice to public policy

Regulators, governments and others have been keen to endorse good risk management practices. For example, the OECD Principles of Corporate Governance published in April 2004:

- Identify a key function of those charged with governance as "ensuring the integrity of the corporation's accounting and financial reporting systems, including the independent audit, and that appropriate systems of control are in place, in particular, systems for risk management, financial and operational control, and compliance with the law and relevant standards (Principle VI.D.7);
- State that disclosure should include material information on "foreseeable risk factors" (Principle V.A.6).

Section 5 of this paper sets out certain EU Member State, European and US regulatory requirements. In the United States, the Sarbanes-Oxley Act of 2002 established new regulatory requirements for internal control for SEC registrants. In the EU, the European Commission is proposing new requirements for listed companies and other public interest entities. Certain national initiatives are set out in the Appendices IV to XXII. Countries for which no appendix has been included may have risk management and internal control requirements for financial institutions and other sectors, but not for companies generally.

As announced in its Action Plan on modernising company law and enhancing corporate governance in the European Union, the European Commission formally established the European Corporate Governance Forum in October 2004 to encourage the coordination and convergence of national codes of corporate governance through regular high-level meetings. The Forum met for the first time in January 2005 and is expected to meet once or twice a year. It comprises representatives from Member States, European regulators, issuers and investors and other market participants and academics.

Regulatory requirements are often imposed on companies as a response to financial scandals and business failures where those charged with governance are perceived to have fallen short. They are seen as a means of consolidating the best practices pioneered by leading companies, forcing others to raise their game and building public trust. However, improvements in business risk management and related disclosure have not been and should not be driven by regulatory requirements alone. Moreover, the introduction of regulatory requirements should be based on proper evidence about the likely costs and benefits.

Emphasis should be placed on the overall need for more research and learning from experience to direct developments in risk management and internal control appropriately.

There is also a need for principles to underpin regulatory developments and Section 3 of this paper sets out overriding principles which are relevant to the introduction of any requirements on risk management and internal control. Many EU Member States have taken initiatives. 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.

2.4. Questions for commentators

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

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.**

3. OVERRIDING PRINCIPLES

3.1. The business case for risk management

Company-wide risk management and internal control are a fundamental basis for the successful running of a business to help it define and achieve its objectives. Consequently, 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.

It also needs to be widely recognised that profits are, in large part, the reward for successful risk-taking. To negate any tendency for risk management and internal control to make management and those charged with governance too risk averse, they should be seen as enabling companies to take risks with more confidence and also to seize and benefit from opportunities that are not part of their business plan. Therefore, the purpose of risk management and internal control is to manage risk, including upside risk or 'the risk of lost opportunities', appropriately rather than to eliminate it. The strong business case for risk management and internal control supports the argument for principles-based requirements which allow for the use of judgement in discharging responsibilities.

3.2. 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 outcomes to be achieved. Requirements should not comprise rigid rules that prescribe how those outcomes are achieved.

If risk management and internal control are seen as ends in themselves there is a danger of 'one size fits all' solutions which ignore the unique aspects of each business and impose bureaucratic requirements whose costs exceed the benefits and which do not enhance confidence. The use of codes and the 'comply or explain' approach are ways of promoting principles rather than detailed rules. Agreement on principles is also important in an EU context because it allows for national variations whilst building confidence across a single market.

The advantages of principles-based or objectives-oriented requirements can be summarised as follows:

- They provide necessary flexibility in a multi-cultural, multi-lingual and multi-jurisdictional environment;
- The changing needs of the public interest can be achieved in a more responsive and effective way through achievement of objectives than through technical compliance with required procedures;
- Internal control and risk management are highly judgemental processes that have to adapt to an infinite range of circumstances. A principles-based approach allows for the use of judgement;
- An approach based on robust principles and objectives allows for responsiveness in complex situations and in the light of new developments;
- For processes to continue to develop there must be room for innovation. Innovation is restricted if people are required to follow procedures which have become out of date.

3.3. 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. Moreover, concentrating on listed companies does not imply either an unwillingness to 'think small first' or a narrow view of governance.

On the first count, it is recognised that many listed companies are small and medium sized entities (SMEs) and that excessive regulatory requirements should not be allowed to drive them from public capital markets or deter such entities from entering capital markets. An emphasis on principle-based requirements should mitigate this risk and FEE supports principle-based standards.

Turning to governance, a focus on listed companies does not imply that FEE is concerned solely with the governance arrangements, including internal control, that support price-sensitive disclosures and financial reports. Whilst this is the focus of US federal securities market legislation such as the Sarbanes-Oxley Act, FEE is interested in the wider issues of accountability covered by company law.

3.4. 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. As external auditors of a company are not charged with its governance, the scope of external auditors' responsibilities cannot exceed the responsibilities assumed by those charged with governance. Consequently, questions about the role of external auditors cannot and should not be addressed before those of the boards and management of companies.

Difficult scope issues, such as how to deal with joint ventures and outsourced activities, should also be dealt with from the point of view of what it is reasonable to expect of those charged with governance of the entity concerned. The presumption is that responsibility needs to be exercised at a group and not just at an individual entity level. However, companies need to be consulted on such issues so that any related requirements are seen as responses to reasonable shareholder expectations rather than as regulatory burdens.

3.5. 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.

Recent scandals have revealed situations in which it appears that investors were not informed about disproportionate levels of risk. However, there is a danger of an overreaction which might discourage the risk-taking that is essential to wealth creation. Wealth creation is about considered risk-taking from the company's point of view and about informed risk-taking from the shareholders' point of view.

Therefore there needs to be an overall evaluation by regulators and investors of the combined effect of internal control requirements, including related standards and guidance, and the liability of those involved. Liability should be appropriately aligned to the level of responsibility taken and should encourage the use of reasonable judgement, useful disclosure and fair enforcement.

3.6. Questions for commentators

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.**

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.**

4. ISSUES TO BE ADDRESSED

4.1. Matrix for analysis

The risk management and internal control activities of a company may be characterised in two ways: firstly by reference to the type of risk involved; and secondly by reference to the type of risk management and internal control activity. This is reflected in the matrix for analysis shown in Figure 1 below.

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			

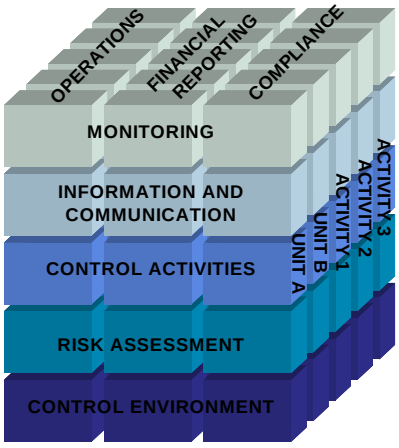
Types of risk are distinguished between those relating to financial reporting objectives, those relating to compliance with laws and regulations affecting the business and those relating to operations and strategy. The latter category is wide and combines external risks relevant to the determination of strategy with operational risks relevant to the execution of strategy. In practice it will often be appropriate to distinguish operational and strategic risks but they are treated together in the current paper.

Principles for each of the two main types of activity identified above – manage risks and disclose - are identified in Sections 4.2 and 4.3 respectively. The potential provision of assurance and audit opinions related to risk management and internal control is separately considered and further explained in Section 6.

4.2. Risk management and internal control principles

As a practical matter, activities related to identifying, evaluating and responding to risks and concluding on the effectiveness of risk management or internal control will need to have regard to an appropriate framework. One of the resultant benefits is that it helps to establish a common language for risk management and internal control and prevents people from talking at cross purposes. An example of a framework is the COSO Framework for internal control represented below. This covers some but not all of the matters included in the matrix shown in Figure 1 above.

Figure 2: COSO Framework



Under the COSO Framework for internal control, there is a direct relationship between objectives, which are what an entity strives to achieve, and the components of internal control, which represent what is needed to achieve the objectives. The process of evaluating an entity's risk management should also take into account the timescale required to perform such a process. The relationship between objectives and components can be depicted by the cube shown above:

- The three COSO objectives categories – operations, financial reporting and compliance – are represented by the vertical columns;
- The five COSO components – monitoring, information and communication, control activities, risk assessment and control environment - are represented by horizontal rows; and
- Business units or activities of the entity are depicted by the third dimension of the matrix.

Other frameworks which build on the COSO framework for internal control are the Canadian CoCo framework and the UK's Turnbull guidance. In September 2004 COSO also published its *Enterprise Risk Management – Integrated Framework* which extends the COSO Framework for internal control to cover risk management and strategic risks.

The US Securities and Exchange Commission (SEC) has recently requested that COSO perform work as a matter of urgency with the aim of issuing a lighter version of its internal control framework for smaller entities. FEE understands that the Canadian Institute of Chartered Accountants (CICA) has no plans to amend or update CoCo.

In the UK, a Review Group set up by the Financial Reporting Council is engaged in a review of the Turnbull guidance issued in 1999. A Consultation Paper was published in December 2004 as part of a wide-ranging evidence gathering phase involving investors and companies and proposals are expected to be exposed for comment in mid-2005 for implementation in 2006.

An appropriate framework is designed to help those charged with governance to analyse their company's risk management and internal control and to provide guidance to management to implement related systems. Frameworks also help management and those charged with governance to reach conclusions on the effectiveness of risk management and internal control systems. Conclusions on effectiveness are useful for promoting improvements, establishing priorities and enforcing accountability. However, the ability of those charged with governance to assess whether a risk management system or specific controls are effective or not is a major challenge.

An issue facing EU regulators and interested parties is whether a common framework should be developed for general application by EU companies in addition to existing frameworks including the three (COSO, Turnbull and CoCo) so far recognised by the SEC for the purposes of compliance with the requirements of Section 404 of the Sarbanes-Oxley Act. A framework would generally only be considered suitable for widespread adoption if it was established following a transparent due process and was kept up to date. It would also be expected to provide:

- Consistency, in the sense that broadly similar risks, tests and conclusions are identified each time the assessment is performed by another individual under similar circumstances with the same sufficient amount of effort; and
- A trail relating to the performance of the assessment which somebody who had not been previously involved in the assessment would be able to follow.

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.

4.3. Disclosure principles

It is possible to disclose specific risks faced by an entity without making any disclosure of how risks are managed and controlled. Indeed as explained later, European directives currently require the disclosure of a company's principal risks but not how they are managed and controlled. As represented in the matrix in Figure 1, this discussion paper considers potential additional disclosure of:

- The overall process of risk management and internal control;
- The management of specific risks; and
- Conclusions about the effectiveness of risk management and internal control or aspects of them.

Disclosure of information about risk management and internal control needs to be useful for decision-making by shareholders exercising rights as shareholders. Specific qualitative characteristics of useful information are generally recognised to include understandability, relevance, materiality, reliability and comparability. The benefits of information displaying these characteristics also need to be balanced against the cost of providing the information.

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

- 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.

The Sarbanes-Oxley Act requires published opinions about the effectiveness of internal control over financial reporting. The Sarbanes-Oxley Act, as an initiative to improve risk management and internal control, results from the US federal securities market legislation system which focuses on financial reporting and disclosures to markets. It does not stem from a company law system empowering shareholders to use disclosures to influence companies to adopt more demanding, but proportionate and cost-effective standards of risk management. This is not envisioned in US state corporation law but is in European company law. A key question facing EU companies, shareholders, regulators and other stakeholders is therefore whether the external disclosure of such effectiveness conclusions provides useful information to shareholders the benefits of which exceed the costs.

Decisions about risk and controls are difficult to communicate succinctly and fairly because they reflect differing risk appetites and involve complex and subjective judgements, for example about the strength of the control environment that is the foundation of internal control. There are also subtle differences between effectiveness statements that depend on whether they relate to the design or operating effectiveness of internal controls and whether they also cover the assessment of risk.

4.4. Questions for commentators

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

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?

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?

5. REGULATORY OPTIONS AND PROPOSALS

5.1. Existing EU and Member State requirements

There are no existing EU requirements related to risk management and internal control. There are however some requirements related to the disclosure of specific risks.

EU directives regulate the contents of the annual report. As a result of the Modernisation Directive, the annual report (referred to as the directors' report in some Member States) must include a fair review of the development and performance of the company's business and of its position, together with a description of the "principal risks and uncertainties" that it faces. The review shall be a balanced and comprehensive analysis consistent with the size and complexity of the business. To the extent necessary for an understanding of the company's development, performance or position, the analysis shall include both financial and, where appropriate, non-financial key performance indicators relevant to the particular business, including information relating to environmental and employee matters.

The Fourth and Seventh Company Law Directives implicitly require companies across the EU to maintain accounting records to enable them to prepare financial statements. Nonetheless, explicit requirements about accounting records and related external reporting obligations for external auditors are left to Member State legislation.

Currently, country requirements for companies to support information for publication in their financial statements and annual reports vary. Different European countries have different regimes to keep accounting records and external auditors are variously required to report explicitly, implicitly or by exception as to whether proper accounting records have been kept or not.

In FEE's view there is a need for a modernised but explicit and broadly stated requirement at EU level to maintain accounting records that support information included in published financial statements. Whilst this would provide a proper foundation for shareholder confidence in financial reporting which is currently lacking at the EU level, it would not represent a requirement related to risk management and internal control over financial reporting.

As is explained further in Section 5.5 there are alternatives to hard and fast legal requirements which can be more efficient in bringing about changes in behaviour, particularly where shareholders have effective powers. Some Member States, such as Cyprus, Germany, Italy and the United Kingdom, already had a variety of mechanisms in place to encourage wider risk management and internal control before recent US scandals. Others, such as Austria, Belgium, Finland, France, Greece, Hungary, Ireland, the Netherlands, Spain, and Sweden are considering or implementing new requirements. European requirements are summarised in Appendices III to XXI.

There is currently a very wide variety of European national regimes for companies and differences in the external auditor's involvement add to the diversity. Such diversity gives rise to additional unproductive costs for those who trade and invest across borders. It will always be necessary to acknowledge national differences in approaches to corporate governance. However, FEE is keen to consider how the matrix for analysis presented in Figure 1 in Section 4.1 could be used to compare requirements for risk management and internal control to identify possible ways to promote an integrated European capital market.

5.2. Sarbanes-Oxley Act requirements

In the United States the response to recent financial scandals has resulted in requirements on listed companies to maintain and report on their evaluation of disclosure controls and procedures and to implement, assess and report on systems of internal control over financial reporting. The requirements of Sections 302 and 404 of the Sarbanes-Oxley Act and the related Auditing Standard No. 2 of the Public Company Accounting Oversight Board (PCAOB) are summarised in Appendix XXII. These developments raise the question of whether the EU should have similar requirements.

This paper is not concerned with the requirements of Section 302 of the Sarbanes-Oxley Act related to SEC-required disclosures although FEE considers that it would be appropriate to introduce an EU requirement reflecting existing Member State requirements for all companies to maintain accounting records that support the information included in published financial statements.

The Sarbanes-Oxley Act requirements of Section 404 in relation to financial reporting controls and related assessments of effectiveness are summarised in Figure 3 below. None of the existing European Member State requirements are identical to the US requirements. They include elements that are not covered by Sarbanes-Oxley. None have any legal requirements which are directly comparable to the Sarbanes-Oxley Act requirements to publicly disclose conclusions regarding effectiveness, albeit only on internal control over financial reporting.

It should be noted that effectiveness of internal control over financial reporting has a specific meaning in the US whereby effectiveness criteria are defined through Auditing Standard No.2 of the PCAOB by reference to material weaknesses.

The standard requires the issuance of an adverse opinion regarding the effectiveness of internal control over financial reporting should one or more material weaknesses arise. A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material financial statement misstatement will not be prevented or detected.

Circumstances presumed to be at least a significant deficiency and a strong indicator of a material weakness include identification by the external auditor of a material misstatement in the year-end financial statements that was not identified by the company's internal controls, even if management subsequently corrects the misstatement prior to issuance of the financial statements and the identification of fraud of "any magnitude on the part of senior management".

Figure 3: Sarbanes-Oxley requirements

			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	✓		

It should be noted that disclosures of specific risks faced by an entity are covered by SEC Management Discussion and Analysis (MD&A) requirements rather than the Sarbanes-Oxley Act.

5.3. Proposed European Directives

Proposals in the Directive on Statutory Audit

The European Commission published proposals for EU requirements on risk management and internal control in 2004 in the form of the proposed Directive on Statutory Audit and proposed amendments to the Fourth and Seventh Directives. These proposals are summarised below, whilst their antecedents in the EC Communication on Company Law and Corporate Governance of May 2003 and the report of the High Level Group of Experts are summarised in Appendix I.

The proposed Eighth European Union Company Law Directive on "the Statutory Audit of Annual Accounts and Consolidated Accounts" (proposed Directive on Statutory Audit) published by the EC on 16 March 2004 and by the Council of the European Union on 7 December 2004 contains proposed requirements for the audit committee of a public interest entity to monitor the effectiveness of the company's internal control, internal audit where applicable, and risk management systems. Overall responsibility for all three remains with the company's management and those charged with governance.

The explanatory memorandum to and Recital (20) of the proposed Directive on Statutory Audit state "that an effective internal control system minimises financial, operational and compliance risks, and enhances the quality of financial reporting."

The memorandum goes on to say that "Such a system requires the maintenance of appropriate policies and processes that ensure a prompt dissemination of reliable information and compliance with applicable laws and regulations, and safeguard the proper use of the company's assets" and that "the function of the audit committee is to monitor that control activities are performed and communication and reporting processes are in place for breaches of internal control policies and applicable laws and regulations. This should by no means undermine the fact that the responsibility for the operation, review and disclosure of the internal control system lies with the board of directors collectively."

The proposed Directive on Statutory Audit contains a requirement for the audit committee of a public interest entity to monitor the effectiveness of the company's internal control, internal audit where applicable, and risk management systems. In view of the references to operational and compliance risks in the explanatory memorandum, it seems as if the audit committee is not only intended to monitor financial reporting risks. On the basis that the requirement to monitor appears to require procedures to have been put in place, the implied matrix for the proposed Directive on Statutory Audit is as shown below:

Figure 4: Proposed Directive on Statutory Audit requirements

			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			

Proposed amendments to the Fourth and Seventh Directives

On 27 October 2004, the European Commission presented a proposal to amend the Fourth and Seventh Company Law Directives. This includes a requirement for all listed EU companies to provide a corporate governance statement in their annual report which would contain "a description of the company's internal control and risk management systems." The recitals to the proposals appear to limit the scope of the requirements to financial reporting, rather than compliance, operational and strategic matters.

Where a listed company prepares a consolidated annual report there would be an additional requirement for a "description of the group's internal control and risk management systems in relation to the process for preparing consolidated accounts."

Bearing in mind the high level nature of the proposed requirements to provide descriptions of internal control and risk management systems, the implied matrix for the proposal to amend the Fourth and Seventh Directives is as set out below:

Figure 5: Proposed Fourth and Seventh Directives requirements

			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			

The Modernisation Directive of 18 June 2003 establishes a requirement to disclose risks but does not go as far as to require disclosure of how they are managed.

5.4. FEE proposals in response to EU initiatives

FEE broadly supports the European Commission approach to introducing requirements in relation to risk management and internal control systems. In particular, FEE broadly welcomes the relevant aspects of the proposed Directive on Statutory Audit and the proposals to amend the Fourth and Seventh Directives and, in particular, the fact that the Commission:

- Is supporting and reinforcing existing best practice amongst listed companies;
- Recognises the importance of disclosure and the monitoring role of the audit committee in bringing about improvements;
- Has refrained from introducing explicit requirements relating to the management of risk which would be at variance with the approach to corporate governance adopted in many Member States; and

- Has not introduced requirements for the disclosure of the management of specific risks which, if not properly debated beforehand, might lead to bland standardised reporting.

FEE has also commented on the proposal to amend the Fourth and Seventh Directives and stated that there is a need to clarify the audit requirements for the corporate governance statement, including any reporting on risk management and internal control, due to the implications of positioning the corporate governance statement in the annual report. FEE has also expressed support for the Commission's recognition that companies themselves are the first line of defence in reporting and auditors the second. The auditor should not provide assurance services in respect of risk management and internal control which are wider in scope than the relevant responsibility of members of a company's administrative, management and supervisory bodies.

However, FEE's support is qualified by the following observations.

- 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.

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

- 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.

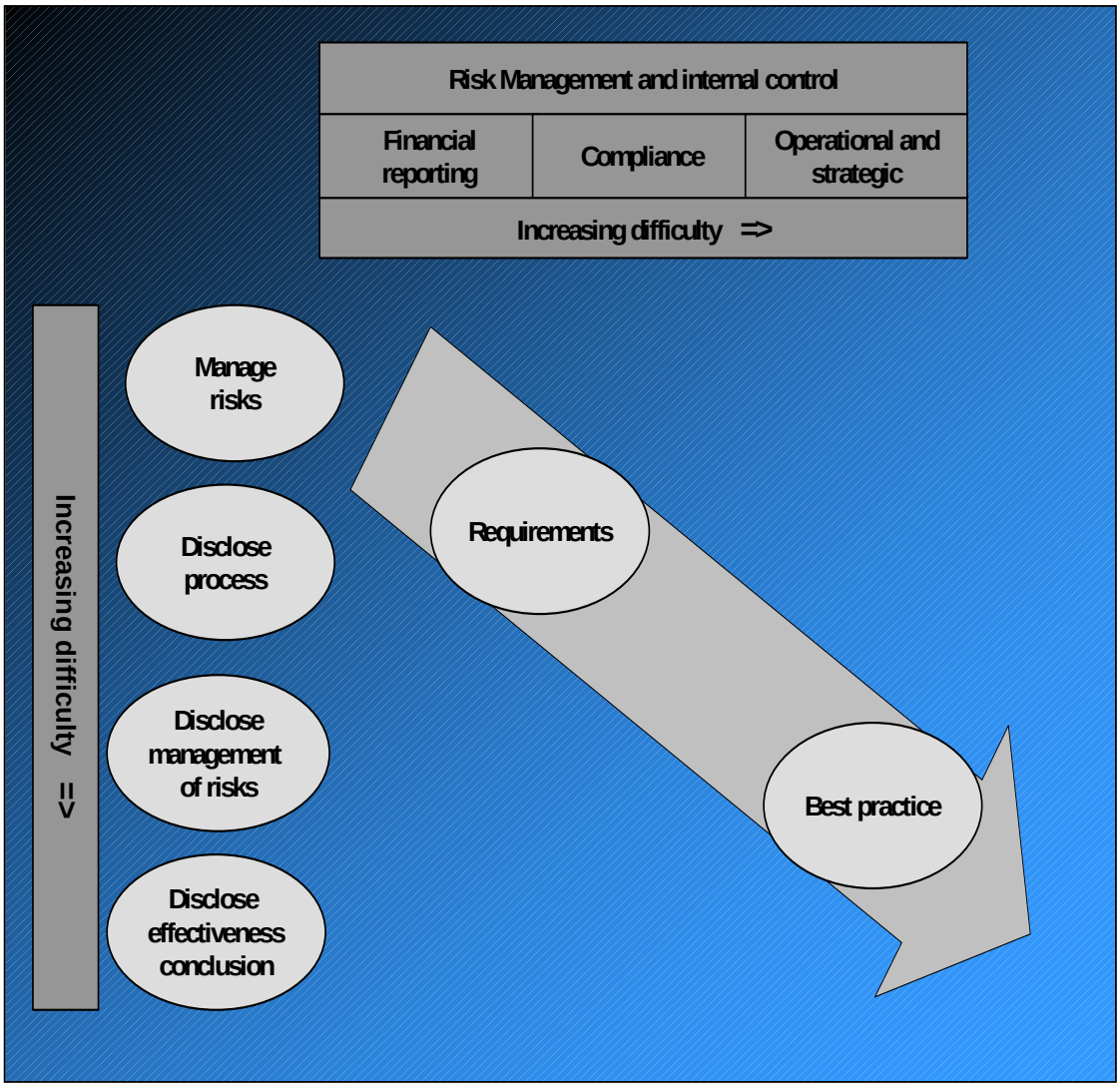
5.5. Issues for further consideration

The basis for a possible evolutionary path to be followed by companies is set out below in Figure 6. This recognises the increasing difficulty and challenges faced by management and those charged with governance as they seek to:

- Manage financial reporting, then compliance and then operational and strategic risks; and
- Disclose first their overall process of risk management and internal control, then their management of risks and finally conclusions on effectiveness.

It is against this backdrop that any regulatory requirements will always need to be foreshadowed by pioneers of best practice.

Figure 6: Charting an evolutionary path



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 which are not generally available to US shareholders under US state corporation law and the strengthening of shareholders' rights is high on the European Commission's agenda.

European shareholders do not necessarily need to look to a European equivalent of US federal securities legislation, such as the Sarbanes-Oxley Act, to bring about improvements in risk management and internal control. Accordingly, FEE welcomes the fact that the European Commission has not rushed to implement an EU equivalent of the requirement in Section 404 of the Sarbanes-Oxley Act for an audited statement from management and an auditor's statement as to whether or not internal control over financial reporting is effective.

It is on the foregoing basis that 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.

Figure 7: FEE issues for consideration by listed companies and regulators

			Types of risk			References
			Financial reporting	Compliance	Operational and strategic	
Types of activity	Manage risks	Identify and evaluate	1	1	1	See 1. Issues related to managing risks
		Respond	1	1	1	
		Conclude on effectiveness	1	1	1	
	Disclose	Overall process	2	2	2	See 2. Issues related to disclosures of overall process
		Management of specific risks	3	3	3	See 3. Issues related to disclosures of management of specific risks
		Effectiveness conclusion	4	4	4	See 4. Issues related to disclosure of effectiveness conclusions

1. Issues related to managing risks

It is widely recognised as best practice for companies to establish systems of risk management and internal control and to strive to extend the scope of these systems across the whole of the business and to reach conclusions on their effectiveness internally within the company. The proposed Directive on Statutory Audit would also require the audit committees of listed companies to monitor such systems.

The significant practical challenges and change management issues that face companies should not be underestimated. 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.

One aspect of organisational change that is likely to be a prerequisite for any formal systems of risk management and internal control will be the company-wide adoption of a framework and language for considering risk and control issues.

2. Issues related to disclosures of overall process

The proposed amendments to the Fourth and Seventh Directives would require listed companies to disclose their overall process of risk management and internal control over financial reporting. Whilst it would be open to companies to disclose that they have no such process, the expectation is that companies would be forced to address the issues raised under item 1 above. Additional issues that arise 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

Whilst there are some requirements in financial reporting standards to disclose how specific financial risks are managed, 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

Given that best practice risk management and internal control involves reaching conclusions internally within the company on effectiveness, it might appear straightforward to disclose these conclusions publicly. A particular benefit of published effectiveness conclusions is that they provide a strong incentive to make better disclosures of overall process and the management of specific risks where there are problems in reaching a positive conclusion. However, 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.

It might nonetheless be possible for those charged with governance to produce meaningful effectiveness opinions in relation to narrower aspects of financial reporting. Such opinions are also only likely to relate to the past, whether at a point in time or for a past period. It will be important for participants in the European discussion of these issues to learn from experience and investor reactions in the United States and current debates in Member States (including the UK, France and Sweden) to see if workable or alternative solutions can be found.

In relation to effectiveness statements, a phased implementation might be considered whereby those charged with governance first acknowledge their responsibility for effectiveness. This could be followed by the preparation and publication of an effectiveness policy statement and processes and procedures to achieve effectiveness and finally the issuance of an annual conclusion on effectiveness.

It might never be reasonable to publish effectiveness opinions in relation to broader types of strategic and operational issues where risk appetites and industry risks differ and cannot reasonably be reduced to a common level.

5.6. Questions for commentators

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?**

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?**

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

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?**

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

6. EXTERNAL ASSURANCE

6.1. Principles for providing assurance services

In this section, assurance is to be understood in the context of an assurance engagement as defined by the International Auditing and Assurance Standards Board (IAASB) and is further explained in Appendix II. The possible scope of assurance engagements related to risk management and internal control can be thought of using the matrix for analysis presented in Figure 1 in Section 4.1.

The overriding principles set out in this paper state that external auditors' provision of assurance services in respect of risk management and internal control can not exceed the responsibilities assumed by those charged with governance as referred to in Section 3.4. This means that external auditors cannot and should not provide assurance services on disclosures beyond those made by companies. It does not necessarily mean that external auditors should obtain assurance and report in relation to all the risk management and internal control activities and disclosures for which those charged with governance are responsible. Ultimately, the perceived benefit of any assurance in enhancing the credibility of company risk management and disclosure needs to exceed the costs.

It is essential that auditors' liability fairly and reasonably relates to the consequences of unsatisfactory audit and assurance performance. The Commission Communication of September 2004 on *Preventing and Combating Corporate and Financial Malpractice* indicates that the first line of defence is the internal control in a company, in particular by board members. The second line of defence is primarily the external auditors. External auditors have to audit the accounts or provide assurance on internal control systems prepared or approved by members of the administrative, management and supervisory bodies of the company. It should be made clear that the group of stakeholders to whom the external auditor is responsible cannot be wider than the group to whom those bodies are themselves responsible.

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.

If external auditors' assurance work is to be extended in relation to risk management and internal control then it would be most natural first to extend their existing work on internal financial control in relation to the audit of the financial statements. Indeed, what is currently expected of auditors of financial statements in relation to risks and internal control will be further increased by ISA 315 *Understanding the Entity and its Environment and Assessing the Risks of Material Misstatement* and ISA 330 *The Auditor's Procedures in Response to Assessed Risks*, issued by the IAASB.

6.2. Role of the external auditor in the proposed Directive on Statutory Audit

As far as external auditors are concerned, the explanatory memorandum to the proposed Directive on Statutory Audit published by the EC and Article 39.4 of the proposed Directive published by the Council of the European Union states that there is an obligation for the external auditor to report to the audit committee on key matters arising from the statutory audit, in particular on material weaknesses of the internal control system in relation to the financial reporting process.

The memorandum also says that the external auditor and the audit committee "should co-operate in the fields of audit and of the financial reporting process. To this extent, the auditor should communicate on a timely basis with the audit committee on those matters of governance interest that arose from the audit of the financial statements." There then follows a list of matters arising from their work on the financial statements which auditors communicate to the audit committee. The list includes:

- Significant risks and exposures facing the company; and
- Material weaknesses in internal control in relation to the financial reporting process.

6.3. Proposed amendments to the Fourth and Seventh Directives

Proposals to amend the Fourth and Seventh Directives to require listed companies to provide a corporate governance statement include a requirement for a description of internal control and risk management systems. The consequences for auditors of the positioning of this statement call for careful consideration.

The proposals to amend the Fourth and Seventh Directives require that for listed companies a corporate governance statement is included as a separate part of the annual report. Inclusion in the annual report will require auditors to verify that the annual report is consistent with the annual accounts for the same financial year.

Some Member States have gone beyond this requirement and made the annual report, which would include the corporate governance statement, subject to a full audit requirement. This is of concern because not all elements of such a statement are objectively verifiable and because this would expand the scope and cost of the statutory financial statement audit. If a full audit requirement is inadvertently imposed as a result of the positioning of the corporate governance statement in the annual report, there will be resistance to further development of corporate governance codes to cover judgemental areas that are important to stakeholders.

As FEE understands that it is not the intention of the European Commission to make the corporate governance statement subject to a full audit requirement but only to consistency verification, this should at least be explained in the recitals to the Directives. This would nevertheless allow Member States that wish to do so to impose full audit requirements for the objectively verifiable parts of the corporate governance statement.

It is advisable that the proposal should also be less prescriptive about the location of the corporate governance statement, only requiring that the corporate governance statement should be submitted to the shareholders together with the annual accounts and the annual report. This would allow those Member States that require the annual report to be subject to full audit to find a solution that suits their reporting and auditing arrangements.

6.4. Relevant international standards

In order for an external auditor to provide assurance services in relation to company reporting requirements on risk management and internal control, standards other than auditing standards are required. In FEE's view, assurance standards issued by the IAASB are suitable for this purpose. The IAASB issued in January 2004 its International Standard on Assurance Engagements, ISAE 3000 *Assurance Engagements on Subject Matters Other than Historical Financial Information*, in conjunction with the *International Framework for Assurance Engagements.*

The subject matter of an assurance engagement as defined in ISAE 3000 can take many forms including systems and processes (e.g. internal controls and IT systems), behaviours (e.g. compliance with corporate governance codes) and non-financial performance information (e.g. indicators of efficiency and effectiveness). Suitable criteria or benchmarks should be set to evaluate or measure the subject matter of an assurance engagement. For example, when reporting on internal control, the criteria may be an established internal control framework or individual control objectives specifically designed for the engagement.

Under ISAE 3000 the external auditor provides a written assurance report containing a conclusion that conveys the assurance obtained as to whether the subject matter conforms in all material respects with the identified criteria. This form of expression conveys reasonable assurance and indicates that the external auditor has obtained sufficient appropriate evidence to reduce assurance engagement risk to an acceptably low level. In broad terms, this is comparable in thoroughness to a financial statement audit.

ISAE 3000 can alternatively be applied to limited assurance engagements where the engagement risk is reduced to a level that is greater than for a reasonable assurance engagement. The result is comparable to a review of interim numbers.

ISAE 3000 reaffirms the importance of company reporting criteria as a prerequisite for assurance engagements and provides a solid base for an open debate about the desirable level of required external auditor involvement and related liability issues. Nevertheless, any debate will inevitably be influenced by recent US developments and pre-ISAE 3000 experience in the EU.

6.5. Alternative assurance approaches

Section 404 of the Sarbanes-Oxley Act requires the SEC to prescribe rules requiring each annual report required by the Securities Exchange Act of 1934 to contain an internal control report, which shall:

- State the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
- Contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

With respect to this required internal control assessment, each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. Such attestation shall be made in accordance with standards for attestation engagements issued or adopted by the PCAOB. Any such attestation shall not be the subject of a separate engagement from the related financial statement audit. By definition, the level of assurance provided in such an integrated audit is reasonable assurance as is the case in all financial statement audits.

The legislative requirement for an integrated audit does not allow consideration of limited assurance engagements, standalone engagements on internal control or engagements to address broader issues of internal control related to compliance, operational or strategic risks.

European experience would also support considering assurance work on internal control as being a part of an audit of financial statements. Currently under national laws and standards governing the financial statement audit there is often either a separate reasonable assurance opinion on control matters or an explicit or implicit limited assurance opinion that is purely a by-product of the work performed for the financial statement audit.

However, the exacting standards that underpin the US integrated triple audit of the financial statements, internal control over financial reporting and management's statement on such internal control are widely seen as making a US-style audit uneconomic for the vast majority of entities that are currently subject to statutory audit in the European Union. If the external assurance work is to be extended to provide a separate opinion on risk management and internal control, then it would be appropriate to do so under a separate assurance engagement including appropriate contractual terms.

Adopting in principle ISAE 3000 would have the advantage that it could be applied to enable external auditors to discharge responsibilities in respect of any of the possibilities envisaged in the matrix for analysis presented in Figure 1 in Section 4.1. A reasonable or limited assurance engagement could be performed on a company's risk management and internal controls, or related disclosures, or effectiveness conclusions. It could also be performed in relation either to financial reporting, compliance or wider operational matters.

The principal constraints would be practical ones that might arise, for example, because of:

- Lack of a framework and of adequate and 'auditable' criteria (e.g. for assessing effectiveness);
- Liability concerns;
- Lack of related requirements on companies; and
- A perceived need for additional standards and guidance.

ISAE 3000 envisages that further ISAEs might be required to deal with specific subject matters such as internal control. For example, further material might deal with the evaluation of criteria and working with specialists especially in areas outside financial reporting.

6.6. FEE proposals

It is important for the auditing profession to take a lead, for example in facilitating the development of criteria for the management of risk, including assessing effectiveness. Nevertheless, it is also important for audit practitioners and standard setters to bring other parties with them and recognise the need for benefits to exceed cost. There is little point in having criteria for the evaluation of internal control and related assurance standards if shareholders do not believe that there is a case for assurance, if companies are not required to apply the criteria and if auditors and those charged with governance of companies face an onerous liability regime.

In summary, FEE makes the following proposals:

- 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 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.

6.7. Questions for commentators

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.

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?

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?

INVITATION TO COMMENT

Answers are invited to the following questions with supporting arguments and examples:

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. (Section 2.4)**

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. (Section 2.4)**

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. (Section 3.6)**

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. (Section 3.6)**

5. **Is the matrix for analysis presented in Figure 1 in Section 4.1 clear and useful? If not, please explain why not. (Section 4.4)**

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? (Section 4.4)**

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? (Section 4.4)**

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? (Section 5.6)**

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? (Section 5.6)**

10. **What role should regulatory requirements play in promoting improvement in risk management and internal control? (Section 5.6)**

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?**

12. **What views do you have on the issues for consideration discussed in Section 5.5? (Section 5.6)**

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. (Section 6.7)**

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? (Section 6.7)**

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? (Section 6.7)**

In addition, do you have any other comments on this discussion paper not covered by the specific questions reproduced above?

Unless otherwise stated, responses will be regarded as being on the public record. Consultees should indicate specifically when their responses should be treated as confidential. Standard disclosures in responses received by e-mail will be disregarded for this purpose.

Comments received will be analysed and used by FEE as a basis for decisions on FEE's next steps.

Comments should be sent by 31 July 2005 by e-mail to hilde.blomme@fee.be or post to:

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

APPENDIX I – DEVELOPMENT OF EUROPEAN COMMISSION PROPOSALS

This appendix provides additional background information on the development and origins of the European Commission's 2004 proposals in relation to risk management and internal control.

The European Commission Communication on Company Law and Corporate Governance of May 2003 took over the recommendation in the report of the High Level Group of Experts chaired by Jaap Winter ("The Winter Report") to require disclosure by listed companies in an annual corporate governance statement of "the existence and nature of a risk management system".

One of the general themes of the Winter Report is that disclosure has a pivotal role in company law. As a regulatory tool, disclosure:

- Enhances accountability for, and transparency of, governance and creates an incentive to renounce structures that are not best practice;
- Meets a key objective of securities regulation to ensure that market participants can participate in the market on an informed basis; and
- Can be more efficient than substantive regulation through more or less detailed rules.

Accordingly, the Winter Report recommended that an annual corporate governance statement should disclose the system of risk management applied by the company, describing the core strategy and activities of the company and the related risks. Where such a system does not exist, this should be disclosed. The collective responsibility of boards would cover not only financial statements but also the corporate governance statement and statements on key non-financial data, such as information on a company's risk management system.

Winter stated however, that introducing a requirement in EU law for listed companies to have a developed system of risk management needs further study. Consequently, there was an explicit commitment to disclosure requirements but not to requirements for the management of risk.

The Winter Report also focused on the internal aspects of auditing practices, in particular on the responsibility of the board for audit. The audit committee, which in practice is usually set up for these purposes, is seen as having a key role to play in the relationship between the management and the external auditor.

To this end, the audit committee should be pivotal in the internal aspects of the audit function and should:

- Monitor the company's internal audit procedures and its risk management system;
- Meet regularly with those who are responsible for the internal audit procedures and risk management system;
- Consider to what extent the findings of the risk management system should be reported in the company's financial statements; and
- Have access to all internal information relevant to performing its role.

The annual corporate governance statement proposed by the European Commission Communication on Company Law and Corporate Governance of May 2003 would, in accordance with the recommendations of the Winter Report, include information on the system of risk management and where such systems do not exist, this would be disclosed under the principle of 'comply or explain'. In respect of disclosures on the composition and operation of the board and its committees, the Communication states that "…proper information is given on the way in which the company has organised itself at the highest level to establish and maintain an effective internal control system".

In addition, the EC Communication of May 2003 on Reinforcing the Statutory Audit in the EU also announced that the European Commission would examine the role that external auditors play in assessing and reporting on internal control systems to identify the need for further initiatives.

APPENDIX II – GLOSSARY OF TERMS

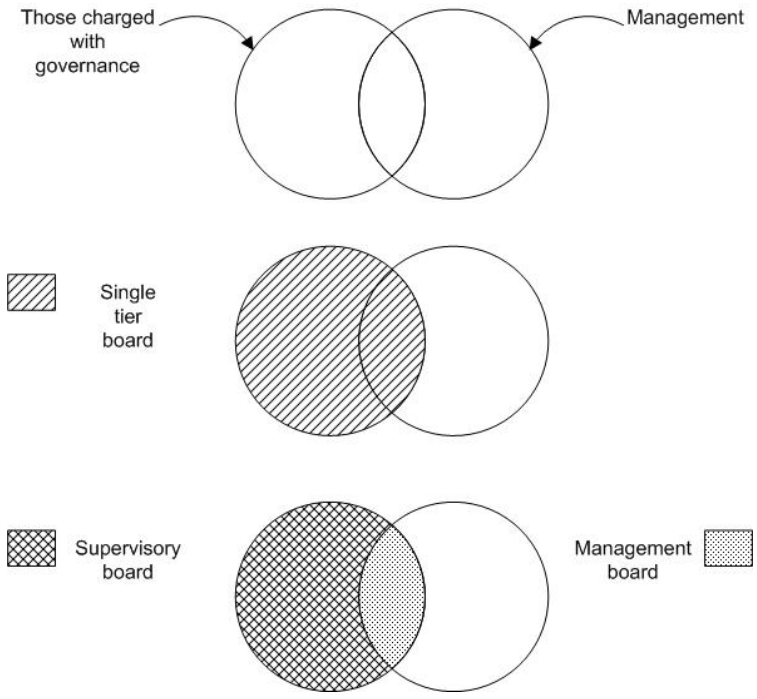
The following explanations are based on those developed by the IAASB.

Internal control: Internal control is the process designed and effected by those charged with governance, management, and other personnel to provide reasonable assurance about the achievement of the entity's objectives with regard to the reliability of financial reporting, effectiveness and efficiency of operations and compliance with applicable laws and regulations. It follows that internal control is designed and implemented to address identified business risks that threaten the achievement of any of these objectives.

Management: Management comprises those who perform senior executive managerial functions and includes persons who are not charged with governance.

Those charged with governance: Those charged with governance is the term used to describe the role of persons entrusted with the supervision, control and direction of an entity. Those charged with governance ordinarily are accountable for ensuring that the entity achieves its objectives, financial reporting, and reporting to interested parties. Those charged with governance include management only when it performs such functions.

In the light of the above explanations, single and two tier board structures may be represented as follows:



Assurance engagement: An engagement in which a practitioner expresses a conclusion designed to enhance the degree of confidence of the intended users other than the responsible party about the outcome of the evaluation or measurement of a subject matter against criteria. The outcome of the evaluation or measurement of a subject matter is the information that results from applying the criteria

to the subject matter. For example, an assertion about the effectiveness of internal control (outcome) results from applying a framework for evaluating the effectiveness of internal control such as COSO (criteria) to internal control, a process (subject matter). Under the *International Framework for Assurance Engagements* there are two types of assurance engagement a practitioner is permitted to perform: a reasonable assurance engagement and a limited assurance engagement.

Reasonable assurance engagement: The objective of a reasonable assurance engagement is a reduction in assurance engagement risk to an acceptably low level in the circumstances of the engagement as the basis for a positive form of expression of the practitioner's conclusion. In an audit engagement, the auditor obtains a high, but not absolute, level of assurance, expressed positively in the auditor's report as reasonable assurance, that the information subject to audit is free of material misstatement.

Limited assurance engagement: The objective of a limited assurance engagement is a reduction in assurance engagement risk to a level that is acceptable in the circumstances of the engagement, but where that risk is greater than for a reasonable assurance engagement, as the basis for a negative form of expression of the practitioner's conclusion.

APPENDIX III: SUMMARY OF RISK MANAGEMENT AND INTERNAL CONTROL IN THE EU AND US [1]

Country	Are there requirements?	Is compliance with requirements mandatory? [2]	Where are the requirements?	Scope of explicit requirements									Framework required?	Specific legal enforcement sanctions?	External auditors' involvement?	Changes under consideration?
				Types of risk?			Types of activities?									
							Manage risks			Disclose						
				Financial reporting	Compliance	Operational and strategic	Identify and evaluate	Respond	Conclude on effectiveness	Overall process	Management of specific risks	Effectiveness conclusion				
Austria	✓	×	Code of Corporate Governance	✓	✓	✓	✓	✓	×	✓	×	×	×	×	✓ Internal report on effectiveness of risk management	×
Belgium	✓	×	Code of Corporate Governance	✓	✓	✓	✓	✓	×	×	×	×	×	×	×	×
Bulgaria	Only for financial institutions	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

[1] All data included in the summary are based on information made available to FEE as at March 2005 which is likely to evolve over time. Compliance with the requirements is voluntary in a significant number of countries. For further details of the data included in the summary, reference should be made to Appendices IV to XXII.
[2] It should be noted that under 'comply or explain' regimes, compliance with specific requirements is not mandatory, but explanations of non-compliance are mandatory.

APPENDIX III: SUMMARY OF RISK MANAGEMENT AND INTERNAL CONTROL IN THE EU AND US [1]

Country	Are there requirements?	Is compliance with requirements mandatory? [2]	Where are the requirements?	Scope of explicit requirements									Framework required?	Specific legal enforcement sanctions?	External auditors' involvement?	Changes under consideration?
				Types of risk?			Types of activities?									
							Manage risks			Disclose						
				Financial reporting	Compliance	Operational and strategic	Identify and evaluate	Respond	Conclude on effectiveness	Overall process	Management of specific risks	Effectiveness conclusion				
Cyprus	✓	✗	Code of Corporate Governance	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓Review and external report on reasonable-ness and consistency of compliance with Code of Corporate Governance	✓ requirements become compulsory for companies listed on Main Market.
Czech Republic	Only for financial institutions	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Denmark	✓	✗	Recommend-ations on good corporate governance	✗	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓

[1] All data included in the summary are based on information made available to FEE as at March 2005 which is likely to evolve over time. Compliance with the requirements is voluntary in a significant number of countries. For further details of the data included in the summary, reference should be made to Appendices IV to XXII.
[2] It should be noted that under 'comply or explain' regimes, compliance with specific requirements is not mandatory, but explanations of non-compliance are mandatory.

APPENDIX III: SUMMARY OF RISK MANAGEMENT AND INTERNAL CONTROL IN THE EU AND US [1]

Country	Are there requirements?	Is compliance with requirements mandatory? [2]	Where are the requirements?	Scope of explicit requirements									Framework required?	Specific legal enforcement sanctions?	External auditors' involvement?	Changes under consideration?
				Types of risk?			Types of activities?									
							Manage risks			Disclose						
				Financial reporting	Compliance	Operational and strategic	Identify and evaluate	Respond	Conclude on effectiveness	Overall process	Management of specific risks	Effectiveness conclusion				
Estonia	Only for financial institutions	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Finland	✓	✗	Corporate Governance Recommend-ation	✓	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗
France	✓	✓	Code of Commerce	✓	✗	✓	✓	✓	✗	✓	✓	✗	✗	Civil action possible and AMF (market regulator) enforcement action	✓ external report	Changes in interpretation and application.
Germany	✓	✓	Stock Corporation Act and Corporate Governance Code	✓	✓	✓	✓	✓	✗	✓	✓	✗	✗	Liability provisions and possibility of misdemean-our	✓ internal reporting	✗

[1] All data included in the summary are based on information made available to FEE as at March 2005 which is likely to evolve over time. Compliance with the requirements is voluntary in a significant number of countries. For further details of the data included in the summary, reference should be made to Appendices IV to XXII.
[2] It should be noted that under 'comply or explain' regimes, compliance with specific requirements is not mandatory, but explanations of non-compliance are mandatory.

APPENDIX III: SUMMARY OF RISK MANAGEMENT AND INTERNAL CONTROL IN THE EU AND US [1]

Country	Are there requirements?	Is compliance with requirements mandatory? [2]	Where are the requirements?	Scope of explicit requirements									Framework required?	Specific legal enforcement sanctions?	External auditors' involvement?	Changes under consideration?
				Types of risk?			Types of activities?									
							Manage risks			Disclose						
				Financial reporting	Compliance	Operational and strategic	Identify and evaluate	Respond	Conclude on effectiveness	Overall process	Management of specific risks	Effectiveness conclusion				
Greece	✓	✓	Corporate Governance Code	✓	×	×	✓	✓	×	×	×	×	×	×	Review – no reporting	×
Hungary	✓	×	Corporate Governance Recommendations - Budapest Stock Exchange	✓	✓	✓	✓	✓	×	✓	×	×	×	×	×	×
Ireland	✓ plus listed companies as U.K.	✓	Companies Acts	×	✓	×	✓	✓	✓	✓	×	×	✓	Investigation by Director of Corporate Enforcement	✓ external reporting	✓
Italy	✓	×	Corporate Governance Code	✓	✓	✓	✓	✓	×	×	×	×	×	×	×	×

[1] All data included in the summary are based on information made available to FEE as at March 2005 which is likely to evolve over time. Compliance with the requirements is voluntary in a significant number of countries. For further details of the data included in the summary, reference should be made to Appendices IV to XXII.
[2] It should be noted that under 'comply or explain' regimes, compliance with specific requirements is not mandatory, but explanations of non-compliance are mandatory.

APPENDIX III: SUMMARY OF RISK MANAGEMENT AND INTERNAL CONTROL IN THE EU AND US [1]

Country	Are there requirements?	Is compliance with requirements mandatory? [2]	Where are the requirements?	Scope of explicit requirements									Framework required?	Specific legal enforcement sanctions?	External auditors' involvement?	Changes under consideration?
				Types of risk?			Types of activities?									
							Manage risks			Disclose						
				Financial reporting	Compliance	Operational and strategic	Identify and evaluate	Respond	Conclude on effectiveness	Overall process	Management of specific risks	Effectiveness conclusion				
Latvia	Only for financial institutions	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Lithuania	✗	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Luxembourg	Only for financial institutions	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Malta	✗	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Netherlands	✓	✗	Corporate Governance Code	✓	✓	✓	✓	✓	✓	✓	✗	✓	COSO indicated as suitable	✗	✗ except for reporting in management letter	✗
Norway	✓	✗	Code of practice for Corporate Governance	✓	✗	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗
Poland	✗	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

[1] All data included in the summary are based on information made available to FEE as at March 2005 which is likely to evolve over time. Compliance with the requirements is voluntary in a significant number of countries. For further details of the data included in the summary, reference should be made to Appendices IV to XXII.
[2] It should be noted that under 'comply or explain' regimes, compliance with specific requirements is not mandatory, but explanations of non-compliance are mandatory.

APPENDIX III: SUMMARY OF RISK MANAGEMENT AND INTERNAL CONTROL IN THE EU AND US [1]

Country	Are there requirements?	Is compliance with requirements mandatory? [2]	Where are the requirements?	Scope of explicit requirements									Framework required?	Specific legal enforcement sanctions?	External auditors' involvement?	Changes under consideration?
				Types of risk?			Types of activities?									
							Manage risks			Disclose						
				Financial reporting	Compliance	Operational and strategic	Identify and evaluate	Respond	Conclude on effectiveness	Overall process	Management of specific risks	Effectiveness conclusion				
Portugal	✓	✓	Stock Exchange Recommendations and Corporate Governance Regulation	✓	✓	✓	✓	✓	✓	✓	×	✓	×	Comply or explain	✓ internal reporting	×
Romania	✓	✓	Companies Law and Stock Market Law	×	✓	×	✓	×	×	×	×	×	×	✓	✓ examine without reporting	✓
Slovak Republic	Only for financial institutions	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

[1] All data included in the summary are based on information made available to FEE as at March 2005 which is likely to evolve over time. Compliance with the requirements is voluntary in a significant number of countries. For further details of the data included in the summary, reference should be made to Appendices IV to XXII.
[2] It should be noted that under 'comply or explain' regimes, compliance with specific requirements is not mandatory, but explanations of non-compliance are mandatory.

APPENDIX III: SUMMARY OF RISK MANAGEMENT AND INTERNAL CONTROL IN THE EU AND US [1]

Country	Are there requirements?	Is compliance with requirements mandatory? [2]	Where are the requirements?	Scope of explicit requirements									Framework required?	Specific legal enforcement sanctions?	External auditors' involvement?	Changes under consideration?
				Types of risk?			Types of activities?									
							Manage risks			Disclose						
				Financial reporting	Compliance	Operational and strategic	Identify and evaluate	Respond	Conclude on effectiveness	Overall process	Management of specific risks	Effectiveness conclusion				
Slovenia	✗	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Spain	✓	✓	Stock Exchange Regulations	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗
Sweden	✓ in future	✓	Corporate Governance Code and Company Law	✓	✗	✗	✓	✓	✓	✓	✗	✓	✗	✗	✓ External reporting	✗
Switzerland	Only for financial institutions	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

[1] All data included in the summary are based on information made available to FEE as at March 2005 which is likely to evolve over time. Compliance with the requirements is voluntary in a significant number of countries. For further details of the data included in the summary, reference should be made to Appendices IV to XXII.
[2] It should be noted that under 'comply or explain' regimes, compliance with specific requirements is not mandatory, but explanations of non-compliance are mandatory.

APPENDIX III: SUMMARY OF RISK MANAGEMENT AND INTERNAL CONTROL IN THE EU AND US [1]

Country	Are there requirements?	Is compliance with requirements mandatory? [2]	Where are the requirements?	Scope of explicit requirements									Framework required?	Specific legal enforcement sanctions?	External auditors' involvement?	Changes under consideration?
				Types of risk?			Types of activities?									
							Manage risks			Disclose						
				Financial reporting	Compliance	Operational and strategic	Identify and evaluate	Respond	Conclude on effectiveness	Overall process	Management of specific risks	Effectiveness conclusion				
United Kingdom	✓	✗	Combined Code and Listing Rules of the UK Listing Authority	✓	✓	✓	✓	✓	✓	✓	✗	✗	Turnbull	✗	✓ external exception reporting	✓
United States	✓	✓	Sarbanes-Oxley Act	✓	✗	✗	✓	✓	✓	✗	✗	✓	COSO, CoCo, Turnbull	SEC enforcement action	✓ external reporting	✗

[1] All data included in the summary are based on information made available to FEE as at March 2005 which is likely to evolve over time. Compliance with the requirements is voluntary in a significant number of countries. For further details of the data included in the summary, reference should be made to Appendices IV to XXII.
[2] It should be noted that under 'comply or explain' regimes, compliance with specific requirements is not mandatory, but explanations of non-compliance are mandatory.

APPENDIX IV – AUSTRIA

Risk Management and Internal Control

1. If there are requirements for companies related to risk management and internal control beyond monitoring accounting systems for preparing financial statements, where are they?
Yes, voluntary only. The requirements are set out in the Austrian Code of Corporate Governance ("the Code"). Compliance with the rules stipulated therein is voluntary. Companies listed on the Prime Market of the Vienna Stock Exchange have to publish a declaration regarding the implementation of the Code (listing requirements since autumn 2004).
2. What is the scope? • **Subject matter / types of risk?**
If companies declare to follow the Code, then Section 66 of the Code requires them to disclose material financial and non-financial risks and the related risk management activities in the Directors' Report (annual report "Lagebericht") which is published together with the annual financial statements. There is, however, no specific reference to internal control in the Code. No specific definition of types of non-financial risk in the Code. Hence, all non-financial risks should be covered.
• **Types of activities?**
Risks should be identified and disclosed. There is no explicit requirement to evaluate and comment on the assessment of the process and the management of specific risks.
3. Is there a framework, and if so which one?
No specific framework.
4. What enforcement and specific legal or similar sanctions are there?
The Code is a voluntary self-regulatory initiative to reinforce the confidence of investors. All listed companies are called upon: (a) To make a public declaration of their commitment to the Code (see 1. above); and (b) To adhere to the rules monitored by an external institution on a regular and voluntary basis and to report on the findings to the public. There are no specific enforcement regulations in place for the Code.
5. What is the involvement of the external auditors, if any, beyond public reporting obligations on financial statements?
Section 78 of the Code states that the auditor shall make a report about the effectiveness of the company's risk management based on the information and documents presented and shall report the findings to the management board. The management board shall bring this report also to the attention of the chairman of the supervisory board.

6. Are Member State changes under consideration?
A proposed new law ("Gesellschaftsrechtsänderungsgesetz 2005") has been passed to the parliament to improve corporate law and to include certain corporate governance issues in the Austrian Company Code; however there are no specific plans in connection with risk management and internal control.

APPENDIX V – BELGIUM

Risk Management and Internal Control

1. If there are requirements for companies related to risk management and internal control beyond monitoring accounting systems for preparing financial statements, where are they?

The requirements are included in the Corporate Governance Code which was published on 9 December 2004. The Code is applicable starting 1 January 2005 for all listed companies on a voluntary basis.

As from 1 January 2006, listed companies should have made public a Corporate Governance (CG) Charter, outlining their corporate governance structure and policies. In the annual report for the year 2005, published in 2006, listed companies will be expected to devote a specific chapter to corporate governance, describing their governance practices during that year and including explanations, where applicable, on deviations from the Code.

2. What is the scope?

- **Subject matter / types of risk?**

The principles based Code identifies the responsibilities of the Board of Directors and the Audit Committee on the level of risk management and the evaluation of the internal control systems.

With respect to its monitoring responsibilities, the Board should:

- Review the existence and functioning of a system of internal control, including adequate identification and management of risks (including those relating to compliance with existing legislation and regulations);
- Take all necessary measures to ensure the integrity of the company's financial statements;
- Review executive management performance;
- Supervise the performance of the external auditor and supervise the internal audit function

The audit committee should:

- Monitor the integrity of the financial information provided by the company, in particular by reviewing the relevance and consistency of the accounting standards used by the company and its group. This includes the criteria for the consolidation of the accounts of companies in the group;
- Review the internal control and risk management systems set up by executive management, with a view to ensuring that the main risks (including those relating to compliance with existing legislation and regulations) are properly identified, managed and disclosed;
- Review the statements included in the annual report on internal control and risk management;
- Review the specific arrangements made, by which staff of the company may, in confidence, raise concerns about possible improprieties in financial reporting or other matters;
- Review the internal auditor's work programme and the effectiveness of the internal audit;
- Monitor the external audit process and the external auditor's independence.

The company should:

- Establish a CG Charter describing all the main aspects of its corporate governance policy;
- State in its CG Charter that it follows the Corporate Governance Principles laid down in this

Code;

- Establish a CG Charter in its annual report describing all relevant corporate governance events that took place during the year under review. If the company does not fully comply with one or more provisions of this Code, it should explain why in the CG Charter of its annual report.

Based on the above, financial reporting, compliance with laws and regulations and operational and strategic risks are covered.

- **Types of activities?**

With respect to its monitoring responsibilities, the board of directors should:

- Review the existence and functioning of a system of internal control, including adequate identification and management of risks (including those relating to compliance with existing legislation and regulations);
- Take all necessary measures to ensure the integrity of the company's financial statements;
- Supervise the performance of the external auditor and supervise the internal audit function.

No assessment of the effectiveness of the internal control structure and/or procedures is required from management or the Board of Directors.

Based on the above, the types of activities covered are managing of risks, including identifying, evaluating and responding to risks as well as disclosure of the overall process of risks.

3. Is there a framework, and if so which one?

There is no framework, nor reference to any existing framework.

4. What enforcement and specific legal or similar sanctions are there?

A declaration on the application of the Corporate Governance Code is required following the 'comply or explain' principle.

There is no specific enforcement regulation in place for the Code.

5. What is the involvement of the external auditors, if any, beyond public reporting obligations on financial statements?

No external auditor's involvement.

6. Are Member State changes under consideration?

No changes are currently under consideration.

APPENDIX VI – CYPRUS

Risk Management and Internal Control

1. If there are requirements for companies related to risk management and internal control beyond monitoring accounting systems for preparing financial statements, where are they?
The requirements are included in the Code of Corporate Governance.
2. What is the scope? • **Subject matter / types of risk?**
Risk management covering the areas of operational, financial, compliance and IT risks. Internal audit services covering all areas of operations. The board of directors should maintain a healthy system of internal controls including financial, operational, as well as compliance controls and risk management. Also companies are required to have audit committees. A healthy system of internal controls generally means one that addresses and minimises risks so as to safeguard shareholders' investments and the company's assets.
• **Types of activities?**
Various activities by listed and non-listed companies. The directors should, at least once a year, conduct a review of the effectiveness of the group's system of internal control and give assurances to shareholders *in their report on corporate governance* that they have done so. This inspection should cover all systems of internal control, including financial, operational, as well as compliance controls and risk management. They should also state in their annual report on corporate governance that the company plans to continue to function as a going concern for the next twelve months. Based on the above, the types of activities covered are managing of risks, including identifying, evaluating and responding to risks as well as internal conclusion on effectiveness; disclosure of the overall process of risks.
3. Is there a framework, and if so which one?
There is no framework, nor reference to any existing framework.
4. What enforcement and specific legal or similar sanctions are there?
Corporate Governance Code – The implementation of the Code is currently voluntary but listed companies have an obligation to include in their board of directors' annual report to shareholders, a report on corporate governance which should state whether the principles of the Code are being implemented. In the first half of the report on corporate governance, the company is required to state whether it applies the principles of the Code. In the second half of the report the company is required to confirm that it has complied with the provisions of the Code and, if it has not, to provide an explanation. There is no specific enforcement regulation in place for the Code.

5.	**What is the involvement of the external auditors, if any, beyond public reporting obligations on financial statements?**
	Generally, external auditors have no major further involvement (subject to below). With respect to the Code of Corporate Governance, the auditor, as part of his review of the reasonableness and consistency of the directors' report, will also review the statement (paragraph) regarding compliance with the Code of Corporate Governance. The auditor is required by law to include a paragraph in the audit report to state whether the information contained therein is consistent with the financial statements. External auditors will also review the parts of the director's report which relate to the continuation of the company as a going concern for the next twelve months.
6.	**Are Member State changes under consideration?**
	Following the Stock Exchange reforms, the Corporate Governance Code will be compulsory for companies listed on the Main Market. The provisions regarding establishment of Audit Committees will also be compulsory for companies listed on the Parallel Market.

APPENDIX VII – DENMARK

Risk Management and Internal Control

1. If there are requirements for companies related to risk management and internal control beyond monitoring accounting systems for preparing financial statements, where are they?

Recommendations on good corporate governance in Denmark issued by the "Nørby Committee" and adopted by the Copenhagen Stock Exchange, which are voluntary.

2. What is the scope?

- **Subject matter / types of risk?**

The recommendations from the "Nørby Committee" detail the purpose of risk management as follows:

- To develop and maintain an understanding within the organisation of the company's strategic and operational goals, including identification of the critical success factors.
- To analyse these possibilities and challenges which are connected with the realisation of the above goals and to analyse the risk of these goals not being met.
- To analyse the most important activities of the company in order to identify the risks attached hereto.

Risk management also focuses on procedures for damage control, the formation of contracts, safety at work, environmental issues and safeguarding physical values. It is recommended that the board ensures that the management establishes efficient risk management systems and that the board continuously follows up on these in order to ensure that they always work efficiently in the light of the company's requirements. As required, but at least once a year, the board should evaluate the company's risk management and by establishing the risk policy, decide on the company's risk-taking including insurance, currency and investment policies.

The risk management system must define the risk and describe how this risk is eliminated, controlled or hedged on a continuous basis.

Based on the above, the types of risks covered are financial reporting and strategy and operations of the company.

- **Types of activities?**

The types of activities covered are managing risks by identifying, evaluating and responding to risks.

3. Is there a framework, and if so which one?

There is no legal reference to a particular framework.

The recommendations from the "Nørby Committee" should be read in the light of several similar codes of conduct from other countries and from international organisations, e.g. COSO and OECD.

4. What enforcement and specific legal or similar sanctions are there?
There are no specific legal sanctions.
5. What is the involvement of the external auditors, if any, beyond public reporting obligations on financial statements?
Following the recommendations of the Nørby Committee, the board should consider how any collaboration with the company's external audit could contribute to the risk management, and to what extent the internal audit could be part of the risk management.
6. Are Member State changes under consideration?
Yes. The recommendations from the "Nørby Committee" are under consideration/revision. Furthermore, some changes might be a consequence of current debate and legislative initiatives in the European Union.

APPENDIX VIII – FINLAND

Risk Management and Internal Control

1. If there are requirements for companies related to risk management and internal control beyond monitoring accounting systems for preparing financial statements, where are they?
The recommendations are included in the Corporate Governance Recommendation for listed companies. The Recommendation is a part of the rules of the Securities Exchange and is intended to be complied with by companies on the Helsinki Exchanges, provided that it is not in conflict with compulsory regulations applicable in the domicile of the company.
2. What is the scope? • **Subject matter / types of risk?**
According to the Corporate Governance Recommendation for listed companies the company shall define the operating principles of internal control, describe the criteria according to which the risk management is organised and describe the manner in which the internal audit function of the company is organised. The purpose of internal control and risk management is to ensure the effective and successful operation of the company, reliable information and compliance with the relevant regulations and operating principles. Internal control helps improve the effective fulfilment of the board's supervising obligation.
• **Types of activities?**
Risk management is part of the control system of the company. The purpose of risk management is to ensure that the risks related to the business operations of the company are identified and monitored. Effective risk management requires definition of the risk management guidelines. For the evaluation of the operations of the company it is important to provide shareholders with sufficient information on risk management. It is also recommended that the significant risks that have come to the knowledge of the board are described. The types of activities covered are managing risks, including identifying, evaluation and responding to risks and the disclosure of the overall process of risk management.
3. Is there a framework, and if so which one?
There is no framework, nor reference to any existing framework.
4. What enforcement and specific legal or similar sanctions are there?
Apart from the principle of comply and explain, there is no specific enforcement regulation in place for the Recommendation.
5. What is the involvement of the external auditors, if any, beyond public reporting obligations on financial statements?
No external auditor's involvement.

6. Are Member State changes under consideration?
No changes are currently under consideration.

APPENDIX IX – FRANCE

Risk Management and Internal Control

1. If there are requirements for companies related to risk management and internal control beyond monitoring accounting systems for preparing financial statements, where are they?
Introduced in the Code of Commerce by the "Loi de sécurité financière" of 1 August 2003 ("law on financial safeguarding"). The Code of Commerce sets the obligation for all corporations (listed or not) and other legal entities if they are listed.
2. What is the scope? • **Subject matter / types of risk?**
The chairman of the board of directors or supervisory board, has to present an annual report to the shareholders (as an appendix to the management report of the board of directors or supervisory board) disclosing (in addition to other requirements) the internal control procedures related to financial reporting.
• **Types of activities?**
The Chairman's report must be descriptive but does not have to be conclusive as to the effectiveness of internal control. In a group of companies, description of procedures should relate to those in force in the consolidating entity, but not at the subsidiary level, and to those relating to the preparation of the consolidation. The Chairman should comment on and describe procedures to "manage" the risks, but does not have to describe the risks themselves. The description of identified risks and how they are addressed is required to be given in the management report accompanying the annual financial statements.
3. Is there a framework, and if so which one?
There is no framework, nor reference to any existing framework. The statutory auditors' institute only makes reference in its recommendation to the general concepts of internal control.
4. What enforcement and specific legal or similar sanctions are there?
Failure to present the annual report (or inadequate information contained therein) constitutes an "irregularity" (not compliance with law) that the statutory auditors must report to the shareholders. A civil action can always be engaged before a court by a shareholder (or investor) who could claim that not producing this report has caused him damage. The market regulator might also engage enforcement actions when a company produces documents for filing.

5. What is the involvement of the external auditors, if any, beyond public reporting obligations on financial statements?

Statutory auditors have to present annually a report to the shareholders (as an appendix to their report on financial statements) stating whether the information contained in the chairman's report is fairly stated, but only for that part of the report dealing with accounting procedures and systems of internal control relating to the preparation of financial statements.

6. Are Member State changes under consideration?

There is no change under consideration in the obligations set by the Code of Commerce stated in very broad terms, but changes might be introduced in their interpretation and thus in their application. Major points under discussion relate to:

- whether the chairman's report should conclude on the effectiveness of procedures and internal control measures,
- whether the chairman's report should also be descriptive of procedures and internal control measures in subsidiary companies.

Those interpretations may change also the content of the statutory auditors' report on internal control.

The AMF (the French regulator) undertook a survey of reports on risk management and internal control issued by listed companies during the last year as a result of the new requirements. The main conclusions of that survey which were made known recently in a public report indicate that for the first year the companies made good efforts to describe in their report the internal control systems and procedures in place, but that there is a great disparity in the way they have reported on the subject and on the content of the reports. The AMF's report further indicates that one of the reasons for this is the absence of a recognized internal control framework which is, on the short term, a handicap for companies to reach a conclusion on the effectiveness of internal control. As a consequence, the AMF is proposing the creation of a working group between the issuers, the auditors and the regulator to work on this subject but also propose to raise this issue at the European level as soon as practicable.

At the present time, and because of those uncertainties and possible changes, the statutory auditors' institute only released a "recommendation" (not a standard) on this subject.

APPENDIX X – GERMANY

Risk Management and Internal Control

1. If there are requirements for companies related to risk management and internal control beyond monitoring accounting systems for preparing financial statements, where are they?

In the law - German Stock Corporation Act (AktG); further clarification in the German Corporate Governance Code (GCGC) , Sec. 4.1.4 for listed companies.

2. What is the scope?

- **Subject matter / types of risk?**

Pursuant to § 91(2) AktG there is an explicit legal requirement for the Management Board of a corporation to take suitable measures – in particular, by establishing a monitoring system – so that developments that may endanger an entity as a going concern are detected early (Risk Early Recognition System).

The GCGC clarifies the overall responsibility of the company to establish a risk management system. This relates to all types of risks affecting the company including financial reporting, compliance and operations.

- **Types of activities?**

Requirement for the Management Board to **implement a risk management system**, especially a risk early recognition system as an important part of the overall risk management of an entity. Risk management should ensure that existing risks are identified, analyzed and evaluated and that risk-related information is systematically forwarded (communicated) to enable the responsible decision-makers within the entity to respond to the identified risks.

The **disclosure** requirements in the German Commercial Code (HGB) – which are specified in the Institut der Wirtschaftsprüfer *(IDW) Accounting Principle 1* – include that the risks of future development be addressed in the **Management Report** (going concern risks and other risks with a material influence on the net assets, financial position and results of operations). The German Accounting Standard GAS 5 "Risk Reporting" - which is, according to § 342 (2) HGB, to be presumed to represent proper accounting principles for consolidated financial reporting - further provides:

- That individual risks and the possible consequences of such risks should be described and – if possible – quantified.

- That the risk management system - including the policies, procedures and organisation - should be described adequately.

There is no requirement for the entity to publish an explicit **conclusion on the effectiveness** of the risk management system. However, according to the German comply-and-explain approach, the Management Board and Supervisory Board of German listed companies are legally required to declare once a year that the German Corporate Governance Code has been and is being adhered to or which of the Code's recommendations have not been or are not being applied. The declaration must be made accessible to stockholders permanently (§ 161 AktG). As the Code states for example, that "*The Management Board ensures appropriate risk management and risk controlling in the enterprise*", a shareholder might deduce only – if at all - an implicit conclusion on effectiveness from

a company's declaration of compliance.

3. Is there a framework, and if so which one?

There is no legal reference to a particular framework. However, the corresponding IDW auditing standard concerning the audit of internal control systems is based on COSO I.

4. What enforcement and specific legal or similar sanctions are there?

Legal provision for liability of the Management Board for damages to the entity.
Possibility of misdemeanour ["Ordnungswidrigkeit"] if an insufficient risk early recognition system leads to incomplete or incorrect disclosures in the Management Report.

5. What is the involvement of the external auditors, if any, beyond public reporting obligations on financial statements?

The scope of external auditor's involvement comprises – in addition to the assessment of the compliance of the bookkeeping system – the description of risks in the Management Report and for listed companies the Risk Early Recognition System as part of the Risk Management System as specified below:

- According to German law (§ 316ff. HGB), the Management Report is also subject to the financial statements audit. The statutory auditor should assess whether the Management Report is consistent with the financial statements and with knowledge obtained by the auditor during the audit, and whether the Management Report as a whole provides a suitable understanding of the position of the enterprise. This includes the assessment whether the risks of future development have been suitably presented.
- For listed stock corporations there is a legal requirement to include the Risk Early Recognition System in the audit of the financial statements and to report thereon in a separate section of the long-form audit report which is addressed primarily to the Supervisory Board (not to the public) to support its governance function. Deficiencies in the measures taken by the Management Board have – as such – no effect on the (short-form) auditor's report. According to § 317 (4) HGB the auditor has to assess whether the Management Board has taken the measures required by law in suitable form and whether the required monitoring system established in accordance therewith is capable of carrying out its functions. These requirements are specified in *IDW Auditing Standard 340*.

6. Are Member State changes under consideration?

The requirements of the EU accounting Directives with respect to financial instruments (inclusion of financial risk management objectives and policies in the annual report) have recently been implemented in German Commercial law. No further changes are currently under consideration.

APPENDIX XI – GREECE

Risk Management and Internal Control

1. If there are requirements for companies related to risk management and internal control beyond monitoring accounting systems for preparing financial statements, where are they?
In law number 3016/2002 on Corporate Governance, articles 6, 7 and 8.
2. What is the scope? • **Subject matter / types of risk?**
All listed companies must have organized an independent internal control system, supervised by non executive members of their board of directors. The types of risks covered relate to financial reporting.
• **Types of activities?**
See above in 2. The types of activities covered are managing risks, including identifying, evaluating and responding to risks.
3. Is there a framework, and if so which one?
There is no framework, nor reference to any existing framework.
4. What enforcement and specific legal or similar sanctions are there?
There are no specific legal sanctions.
5. What is the involvement of the external auditors, if any, beyond public reporting obligations on financial statements?
In the legislation regarding the auditors and the auditing profession it is mentioned that the auditor investigates whether there is an internal control system, adequately operating, according to the Presidential Decree 226/1993 article 16.2a.
6. Are Member State changes under consideration?
No changes are currently under consideration.

APPENDIX XII – HUNGARY

Risk Management and Internal Control

1. If there are requirements for companies related to risk management and internal control beyond monitoring accounting systems for preparing financial statements, where are they?

In February 2004 the Budapest Stock Exchange issued its Corporate Governance Recommendations. Compliance with the recommendations is recommended but not mandatory for companies listed on the stock exchange.

Listed companies, however, will be required to publish a declaration on their corporate governance practices, comparing those to the Recommendations. Companies listed in category A will be required to make the declaration for their 2004 business year for the first time. For category B companies the first declaration is due after their 2005 business year.

2. What is the scope?

- **Subject matter / types of risk?**

The board of directors shall ensure the integrity of financial and accounting reports and define guidelines for ensuring transparency of operations and for disclosure of corporate information.
The board of directors shall disclose the risk management guidelines ensuring that all risks of essential internal and external operations, financial and legal compliance and other risks are evaluated and managed adequately by a stable internal mechanism. The disclosure shall include the review of adopted risk management policy and main areas of risk management. It is the Board of Director's responsibility to provide information to shareholders, at least once a year in the annual report, on the risk factors relevant to the Company's operations and business activities."

Based on the above, the risks covered are financial reporting, compliance and operations.

- **Types of activities?**

The board of directors is responsible for defining risk management guidelines to ensure that risk factors are identified and that internal control mechanisms are in place to manage (identify and evaluate) those risks.

The board shall also ensure that management sets up a system of internal controls which ensures that the company's objectives are met.

An independent internal audit group shall be established which reports to either the board of directors or to the supervisory board on areas of risk management, internal control and corporate governance.

The audit committee supervises effectiveness of risk management, of the operations of the system of internal controls and of the activities of internal audit.

The board shall disclose its risk management policies (overall process only).

3. Is there a framework, and if so which one?

There is no framework, nor reference to any existing framework.

4. What enforcement and specific legal or similar sanctions are there?
Companies will have to apply the 'comply or explain' principle with respect to the issues covered by the Corporate Governance Recommendations. There is no specific enforcement regulation in place for the Code.
5. What is the involvement of the external auditors, if any, beyond public reporting obligations on financial statements?
No external auditor's involvement.
6. Are Member State changes under consideration?
No changes are currently under consideration.

APPENDIX XIII – IRELAND

Risk Management and Internal Control

1. If there are requirements for companies related to risk management and internal control beyond monitoring accounting systems for preparing financial statements, where are they?

Listed companies – Combined Code on Corporate Governance ("Code")

Listed companies and private companies - with the exception of a private limited liability company whose balance sheet total does not exceed €7.618 million and whose turnover does not exceed €15.237 million (two of the three criteria used in determining medium-sized companies). Section 205E, Companies Act, 1990 ("1990 Act") – Not yet in force, see 6 below.

2. What is the scope?

- **Subject matter / types of risk?**

Code – System of internal controls.

1990 Act:

- Policies in relation to compliance with obligations under law.
- Internal financial and other procedures in place to secure this compliance.

- **Types of activities?**

Code - The Code's main principle in relation to internal control states

"The board should, at least annually, conduct a review of the effectiveness of the group's system of internal controls and should report to shareholders that they have done so."

1990 Act - A directors' compliance statement, approved by the Board and to be reviewed at least triennially, shall specify:

- The company's policies in relation to compliance with its obligations under the Companies Acts, tax law, and "…any other enactments…that may materially affect the company's financial statements."
- The internal financial and other procedures in place to secure such compliance.
- The arrangements for implementing and reviewing the effectiveness of such policies and procedures.

A further statement must be included in the Directors' Report annually:

- Acknowledging directors' responsibility for securing the company's compliance with its relevant obligations,
- Confirming that the company has internal financial and other procedures in place that are designed to secure compliance there with or, if not, why, and
- Confirming that the directors have reviewed the effectiveness of the procedures referred to above during the financial year, and, if not, why.
- Specifying whether, based on the foregoing procedures and their review of them, the directors are of the opinion "that they used all reasonable endeavours to secure the company's compliance

with its relevant obligations in the financial year to which the annual report relates". If not, the statement must give the reasons.

- The overall process and risk management is discussed within the Compliance Policy Statement which must be reviewed at least every three years and, if then necessary, revised.

3. Is there a framework, and if so which one?

Code – Internal Control: Guidance for Directors on the Combined Code ("Turnbull")

1990 Act – No reference to a framework. However, the Act clarifies that procedures are considered to be designed so as to secure compliance and to be effective if they provide reasonable assurance of compliance in all material respects.

4. What enforcement and specific legal or similar sanctions are there?

Code – Non-compliance can be enquired into by the Irish Stock Exchange

1990 Act – Non-compliance can be investigated by the Director of Corporate Enforcement

5. What is the involvement of the external auditors, if any, beyond public reporting obligations on financial statements?

Code - The APB Bulletin 'The Combined Code: requirements of auditors under the Listing Rules of the Irish Stock Exchange', revised in December 2004, states that the objective of the external auditors' review is to assess whether the company's summary of the process the board has adopted in reviewing the effectiveness of the system of internal control, is both supported by the documentation prepared by or for the directors and appropriately reflects that process.

1990 Act - The auditors are required by Section 205 F, Companies Act, 1990 to review both directors' compliance statements referred to above and

"…to determine whether, in the auditor's opinion, each statement is fair and reasonable having regard to information obtained by the auditor, or by an affiliate of the auditor within the meaning of section 205D, in the course of and by virtue of having carried out audit work, audit-related work or non-audit work for the company.".

The review report issued by the external auditor is a public report.

6. Are Member State changes under consideration?

Directors

Revised guidance on the ramifications of these statutory obligations has been developed by a group organised by the Director of Corporate Enforcement and issued under the title "Guidance on the Obligation of Company Directors to Prepare Compliance Policy and Annual Compliance Statements under the Companies (Auditing and Accounting) Act 2003"

The Director of Corporate Enforcement has indicated that the relevant sections of the 2003 Act are likely to be brought into force (his recommendation which is subject to Ministerial decision) for accounting periods commencing on or after 1 July 2005. The related statutory requirements covering auditors reporting on those compliance statements and corporate governance matters, such as establishment of audit committees, are likely to be brought into force at the same time.

Auditors

Auditors of companies subject to these statutory provisions must undertake an annual review of the Compliance Policy Statement and the Annual Compliance Statement. A proposed Bulletin giving guidance on how auditors would carry out the review of both compliance statements has been prepared by the Auditing Practices Board in conjunction with the Consultative Committee of Accountancy Bodies – Ireland and the Office of the Director of Corporate Enforcement. Finalisation and publication of this guidance must await movement/decision on the "directors' guidance" referred to above.

APPENDIX XIV – ITALY

Risk Management and Internal Control

1. If there are requirements for companies related to risk management and internal control beyond monitoring accounting systems for preparing financial statements, where are they?

The Corporate Governance Code was issued in October 1999 by Borsa Italiana SPA and is also known as the "Preda Code". It was revised in 2002. The code is voluntary for listed Companies.

In 2001, some fundamental corporate governance rules of the "Preda Code" became compulsory for companies listed in the "S.T.A.R. segment" (Segmento Titoli Alti Requisiti – high qualified security segment).

2. What is the scope?

- **Subject matter / types of risk?**

In the "Preda Code" there is a general reference to risk management and internal control in articles 9.1 and 9.2 (internal control):
"The internal control system is the set of processes serving to monitor the efficiency of the company's operations, the reliability of financial information, compliance with laws and regulations, and the safeguarding of the company's assets.
The board of directors is responsible for the internal control system; it shall lay down the guidelines for the system, periodically check that it is adequate and working properly, and verify that the main risks facing the company are identified and managed appropriately."

- **Types of activities?**

In the "Preda Code" there is a general reference to the activities which must be carried out by the Board of Directors in articles 9.3 and 9.4 (internal control):
"The managing directors:

- Shall identify the main risks the company is exposed to and submit them to the board of directors for its examination;
- They shall implement the guidelines laid down by the board of directors for the planning, operation and monitoring of the internal control system and;
- Shall assign one or more persons to be in charge of the internal control system and provide them with appropriate resources.

The persons assigned to be in charge of the internal control system:

- Shall not be placed hierarchically under a person responsible for operations and;
- Shall report on their activity to the managing directors and to the internal control committee (provided for in Article 10 of the Preda Code) and the members of the board of auditors (Collegio Sindacale)".

The internal control committee is the formally constituted body able to make autonomous and independent assessments vis-à-vis both:

- The managing directors, for issues concerning the safeguarding of the company's integrity, and;
- The auditing firm, for the results set out in the auditors' report and their letter of suggestions.

This explains the composition of the committee, which must be made up of a majority of independent directors and, where the company is controlled by another listed company, exclusively of independent directors.

Consistently with the functions of the committee, provision is also made for the chairman of the board of statutory auditors (Collegio Sindacale) or another auditor appointed by the same to participate in its meetings in representation of the control body provided for in the bylaws.

The managing directors may also participate in the internal control committee since they are empowered to intervene in the matters examined and to identify adequate measures to tackle potentially critical situations.

The list of the committee's tasks is not exhaustive since the board of directors may decide, in the light of the company's nature and the particular types of risk incurred in its entrepreneurial activity (consider banks and insurance companies), to entrust other tasks to the committee.

For listed companies, the board of statutory auditors (Collegio Sindacale) is in general terms required to oversee the following:

- The adequacy of the corporate structure for matters falling within its scope of responsibilities, such as the systems of internal control, the accounting system, and the reliability of these systems to properly record and reflect transactions in the accounting system.

The separation of the audit of accounts function was accompanied by the attribution to the Board of a more strategic and qualified function – that of assessing the general adequacy of the internal structure and accounting system to reflect the companies' acts, facts and assets. However, there is no direct reference to risk management.

Based on the above, the types of activities covered are managing of risks, including identifying, evaluating and responding to risks.

3. Is there a framework, and if so which one?

There is no framework, nor reference to any existing framework.

4. What enforcement and specific legal or similar sanctions are there?

There are no specific legal sanctions.

5. What is the involvement of the external auditors, if any, beyond public reporting obligations on financial statements?

There is no external auditor's involvement. External auditor for listed companies is an independent external audit firm registered on the special roll of the Italian regulator CONSOB which is involved in the audit of accounts of listed companies.

6. Are Member State changes under consideration?

No changes are currently under consideration.

APPENDIX XV – THE NETHERLANDS

Risk Management and Internal Control

1. If there are requirements for companies related to risk management and internal control beyond monitoring accounting systems for preparing financial statements, where are they?
Within the Corporate Governance Code.
2. What is the scope? • **Subject matter / types of risk?**
The company shall have an internal risk management and control system that is suitable for the company. It shall, in any event, employ as instruments of the internal risk management and control system: (a) Risk analyses of the operational and financial objectives of the company; (b) A code of conduct which should, in any event, be published on the company's website; (c) Guides for the layout of the financial reports and the procedures to be followed in drawing up the reports; and (d) A system of monitoring and reporting. The types of risks covered are financial reporting, operations and also implicitly compliance with laws and regulations as this is a management responsibility.
• **Types of activities?**
The management board shall declare in the annual report that the internal risk management and control systems are adequate and effective and shall provide clear substantiation of this. In the annual report, the management board shall report on the operation of the internal risk management and control system during the year under review. In doing so, it shall describe any significant changes that have been made and any major improvements that are planned, and shall confirm that they have been discussed with the audit committee and the supervisory board. The management board shall, in the annual report, set out the sensitivity of the results of the company to external factors and variables. Based on the above, the types of activities covered are managing of risks, including identifying, evaluating and responding to risks as well as internal conclusion on effectiveness; disclosure of the overall process of risk management and external effectiveness conclusions.
3. Is there a framework, and if so which one?
COSO is indicated as a suitable framework, other frameworks would be possible as well.
4. What enforcement and specific legal or similar sanctions are there?
Companies should comply or explain.

5. What is the involvement of the external auditors, if any, beyond public reporting obligations on financial statements?
No external auditor's involvement required except for reporting on internal control to the audit committee and the supervisory board included in the management letter.
6. Are Member State changes under consideration?
No changes are currently under consideration.

APPENDIX XVI- NORWAY

Risk Management and Internal Control

1. If there are requirements for companies related to risk management and internal control beyond monitoring accounting systems for preparing financial statements, where are they?
In the Norwegian Code of Practice for Corporate Governance which was issued on 7 December 2004. Listed companies are expected to apply the Code of Practice with effect from the 2005 financial year.
2. What is the scope? • **Subject matter / types of risk?**
The Code of Practice clarifies the responsibilities of the board of directors in respect of internal control. A listed company's internal control arrangements must at the very least address the organisation and implementation of its financial reporting.
• **Types of Activities?**
The board of directors of a listed company must ensure that the company has good internal control in accordance with the regulations that apply to its activities, including the company's own corporate values and ethical guidelines. The board of directors of a listed company should provide information in the Corporate Governance Statement on how the company's internal control procedures are organised.
3. Is there a framework, and if so which one?
There is no framework, nor reference to any existing framework.
4. What enforcement and specific legal or similar sanctions are there?
Adherence to the Code of Practice is based on the "comply or explain" principle whereby listed companies will be expected to either comply with the Code of Practice or explain why they have chosen an alternative approach. There is no specific enforcement regulation in place for the Code.
5. What is the involvement of the external auditors, if any, beyond public reporting obligations on financial statements?
No external auditor's involvement.
6. Are national changes under consideration?
No changes are currently under consideration.

APPENDIX XVII – PORTUGAL

Risk Management and Internal Control

1. If there are requirements for companies related to risk management and internal control beyond monitoring accounting systems for preparing financial statements, where are they?
The CMVM (stock-exchange regulator for the listed entities) has issued some standards and recommendations, insisting on the establishment of tight internal control mechanisms for detection of risks. CMVM – Corporate Governance Regulation 07/2001
2. What is the scope? • **Subject matter / types of risk?**
For listed entities, the Corporate Governance Regulation recommends the implementation of an internal control system for an effective detection of risks (financial, environmental, legal or others connected to the company's activity and safeguard of its property). More specifically, the board of directors should maintain an effective system of internal controls including financial, operational, as well as compliance of controls and risk management. All listed companies are required to be audited by a statutory auditor.
• **Types of activities?**
All listed entities have to issue annually a Corporate Governance Report where the risk control systems are explained in a general way (Regulation of CMVM 07/2001). The Corporate Governance Report has to include a description of the internal procedures adopted for risk control in the activity of the entity, namely the existence of internal units dedicated to internal audit and risk management. The types of activities covered are managing of risks, including identifying, evaluating and responding to risks as well as internal conclusion on effectiveness; disclosure of the overall process of risk management and external effectiveness conclusions.
3. Is there a framework, and if so which one?
No specific framework is mentioned.
4. What enforcement and specific legal or similar sanctions are there?
No specific enforcement measures are in place. The regulation is built on the principles of comply or explain.
5. What is the involvement of the external auditors, if any, beyond public reporting obligations on financial statements?
There are the general audit standards (DRA 400 – Risk Assessment and DRA 410 – Internal Control) that cover all types of entities and that require the auditor to make a risk assessment of the company and also to report internally to the company on the weaknesses in the internal control system.

6. Are Member State changes under consideration?
No changes are currently under consideration

APPENDIX XVIII – ROMANIA

Risk Management and Internal Control

1. If there are requirements for companies related to risk management and internal control beyond monitoring accounting systems for preparing financial statements, where are they?

- Companies Law no. 31
- Law 297 regarding Stock Markets in Romania

Listed Companies and Stock Market Intermediaries

Obligation by the Stock Market Law (29 June 2004) to have a specially designed internal control department with the specific task of identifying the risks associated with the Company and any departures from the provisions of the special regulations governing listed companies.

Other (than banks and insurance) Companies

The Companies Law expresses the obligation for administrators to ensure that procedures are put in place to protect the assets and to exercise control over the activities and transactions made by the entity. Statutory auditors should ensure also such provision through audit controls. However, a special internal control department is not specially mentioned.

2. What is the scope?

- **Subject matter / types of risk?**

The types of risks covered are mainly compliance with laws and regulations. More specifically, it is mainly risks related to legality of the activities and transactions performed by the entity and protection of assets.

- **Types of activities?**

The type of activity covered is identifying and evaluating risks.

3. Is there a framework, and if so which one?

There is no framework, nor reference to any existing framework.

4. What enforcement and specific legal or similar sanctions are there?

Through the respective laws and regulations (see 1).

5. What is the involvement of the external auditors, if any, beyond public reporting obligations on financial statements?

For Stock Exchange Companies, the external auditors should examine the internal control department activity and supplementary reports.

6. Are national changes under consideration?
Further regulations are expected which should be designed to regulate internal control.

APPENDIX XIX – SPAIN

Risk Management and Internal Control

1. If there are requirements for companies related to risk management and internal control beyond monitoring accounting systems for preparing financial statements, where are they?
All listed companies have to issue annually a Corporate Governance Report (Orden ECO3722/2003 updated and modified by the Circular 2/2004 March 2004 of the CNMV (the stock exchange regulator))
2. What is the scope? • **Subject matter / types of risk?**
The Corporate Governance Report explains the risk control systems in a general way, mainly covering business operations, and the degree of adherence to existing recommendations on Corporate Governance (i.e. Aldama Report). That means a brief explanation on the systems to control the activities developed by the Company as well as identification and description of processes designed to guarantee compliance with laws and regulations.
• **Types of activities?**
Information required on risk control system is as follows: • Generic description of the risk policy of the company, identifying and evaluating which risks are being converted by the system and the adequacy of these systems to the risk profile. • Control Systems established to evaluate, mitigate or reduce main risks. • Circumstances that have motivated the existence of risks and if the systems to mitigate them have worked effectively. • In case of existence of a committee or other group in charge of establishing and monitoring the controls, detail of their activities. • Identification and description of processes designed to guarantee compliance with laws and regulations. Based on the above, the types of activities covered are managing of risks including identifying, evaluating and responding to risks as well as the disclosure of the overall process and management of specific business risks.
3. Is there a framework, and if so which one?
There is no framework, nor reference to any existing framework.
4. What enforcement and specific legal or similar sanctions are there?
There are no specific legal sanctions except for economic sanctions.
5. What is the involvement of the external auditors, if any, beyond public reporting obligations on financial statements?
No external auditors' involvement required.

6. Are Member State changes under consideration?
No changes are currently under consideration.

APPENDIX XX – SWEDEN

Risk Management and Internal Control

1. If there are requirements for companies related to risk management and internal control beyond monitoring accounting systems for preparing financial statements, where are they?

A new Corporate Governance Code (the Code) finalized and issued in December 2004 requires the Board of listed companies to compile a special report on internal control.

The Code will be binding for all listed companies through their contracts with the Stockholm Stock Exchange. It is expected that the Code will be implemented on July 1, 2005 starting with the larger listed companies. As a next step the Code is expected to be in force for all listed companies regardless of size. The detailed implementation plan is yet to be decided.

The Code is built on the principles of comply or explain and includes many other measures apart from the requirements regarding internal control.

2. What is the scope?

- **Subject matter / types of risk?**

The report on internal control by the Board should cover:

i) How the internal control relating to the financial reporting is organized, and
ii) The effectiveness of the internal controls for the most recent fiscal year (related to financial reporting).

- **Types of activities?**

The report from the Board is to be issued annually.

The Code (self regulation) states that it is the responsibility of the Board to make sure that the Company has good internal controls, and to be informed on and evaluate the status of the system of internal controls. The Companies Act (law) states that it is the responsibility of the Board to make sure that the bookkeeping, the management of funds, and other financial aspects of the Company is under sufficient control.

3. Is there a framework, and if so which one?

No specific framework for the internal control or the reporting is mentioned in the Code. Special guidance is to be produced as a joint effort between listed companies and the Swedish Institute (FAR).

4. What enforcement and specific legal or similar sanctions are there?

The Code is built on the principles of comply or explain. It is expected that the market forces will make this work. Currently no specific enforcement measures have been decided. There is no planned regulatory intervention if inadequate controls are reported.

5. What is the involvement of the external auditors, if any, beyond public reporting obligations on financial statements?
The external auditors have to review the Board's report on internal control and issue a separate report. Guidance for this reporting will be developed by the Swedish Institute, FAR. Both the Board's and the auditors´ report on internal control have to be made public, either together with the annual report document (note that they are not a formal part of the statutory annual report) or separately.
6. Are Member State changes under consideration?
No other changes are currently under consideration.

APPENDIX XXI – UNITED KINGDOM

Risk Management and Internal Control

1. If there are requirements for companies related to risk management and internal control beyond monitoring accounting systems for preparing financial statements, where are they?
Appended to the Listing Rules of the UK Listing Authority (which apply to companies that are on the 'official list' of the London Stock Exchange) is the Combined Code on Corporate Governance. Companies have to state how they have applied the Code principles and whether or not they have complied with Code provisions. It they do not comply, they have to explain why not ('comply or explain').
2. What is the scope? • **Subject matter / types of risk?**
Code principle C.2 states that "The board [of directors] should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets." All types of risk. Code provision C.2.1 states that "the board should, at least annually, conduct a review of the effectiveness of the group's system of internal controls and should report to shareholders that they have done so. The review should cover all material controls, including financial, operational and compliance controls and risk management systems."
• **Types of activities?**
Boards, senior management and other employees have to identify, evaluate and manage the risks to the achievement of a company's objectives. The management of risks includes having effective systems of internal control in place within the company. This is a continuous process and should be part of the normal management and business procedures within a company. Reporting: Annually boards have to disclose that there is an ongoing process for identifying, evaluating and managing the significant risks faced by the company, that it has been in place for the year under review and up to the date of approval of the annual report, that it is regularly reviewed by the board and, most significantly, that it accords with the Turnbull guidance. Boards have to conclude on the effectiveness of their systems of internal control. There is, however, no requirement to make a public statement on their conclusions. Boards may wish to provide additional information to assist understanding of the company's risk management processes and system of internal control.
3. Is there a framework, and if so which one?
The Turnbull guidance issued in September 1999. The official title of the report is 'Internal Control – Guidance to Directors on the Combined Code'. The Turnbull guidance is intended to be an aid to better performance by companies as well as being used to demonstrate compliance with the requirements of the Combined Code.
4. What enforcement and specific legal or similar sanctions are there?
There are legal sanctions under the Companies Act for failure to keep proper accounting records. Listed companies are required to follow the rules of the Listing Authority and the comply or explain

requirements of the Combined Code. The internal control aspects of the Combined Code do not attract specific legal sanctions.

5. How are external auditors involved beyond public reporting obligations on financial statements?

Yes. Auditing Practices Board (APB) Bulletin 2004/3 requires external auditors to assess (by way of a review not an audit) whether the disclosures of the board's summary of the process it has applied in reviewing the effectiveness of the system of internal control is both supported by documentation and appropriately reflects the auditors' understanding of the process undertaken by the board. They will relate the statement made by the board to their knowledge of the company obtained during their audit of the financial statements. The scope of the board's review is wider than that of the external auditors.

Reporting by exception: If the auditors conclude:

(a) That the board's summary of the process it has applied in reviewing the effectiveness of internal control is either not supported by or does not appropriately reflect the auditors' understanding of the process undertaken.
(b) That the processes disclosed to deal with material internal control aspects of significant problems disclosed in the annual report and accounts do not appropriately reflect the auditors' understanding of the process undertaken.
(c) That no disclosure has been made by the board that it has failed to conduct a review of the effectiveness of internal control.
(d) Where the board discloses that it has not reviewed the effectiveness of internal control, that its explanation is not consistent with the auditors' understanding; or
(e) That no disclosure has been made by the board that a material joint venture or associated company has not been dealt with as part of the group

Then they report this in the opinion section of their external report on the financial statements.

However, as this does not give rise to a qualified audit opinion on the financial statements the APB recommends that the auditors' comments be included under the heading 'other matter'.

6. Are Member State changes under consideration?

Yes, for directors. No, for external auditors.

On 13 July 2004, the Financial Reporting Council (FRC) announced a review of the continued appropriateness of the Turnbull guidance. Details can be found at www.frc.org.uk/corporate. The Turnbull Review Group (TRG) is chaired by Douglas Flint (Group Finance Director of HSBC Holdings plc). The first phase of the review will first gather evidence from investors, companies and others and the second phase will be the publication of proposals for the revised guidance. Both phases will be the subject of a public consultation process. The first evidence gathering consultation ended on 2 March 2005.

The TRG wants to ensure that the resulting guidance and disclosures provide a framework that is effective and proportionate. When considering possible changes to the current guidance, the Review Group will pay particular attention to the potential impact of such changes on:

- The ability of companies to achieve better their business objectives;
- The ability of investors to make better informed decisions;

- Improving confidence in corporate reporting and governance;
- The balance of costs and benefits; and
- The perceived impact on litigation risk and liability.

The TRG will also be mindful of broader concerns such as the ability of companies to recruit directors and the overall regulatory burden, particularly on smaller listed companies.

The second consultation paper will be issued in mid-2005. The FRC intends that revised guidance will take effect for accounting periods commencing on or after 1 January 2006.

The mandatory Operating and financial Review (OFR) that comes into effect from 1 April 2005 will require listed companies to make disclosures on the principal risks facing the company (or group). The TRG will also be considering how the proposals for the OFR will link with its work.

APPENDIX XXII – UNITED STATES

Risk Management and Internal Control

1. If there are requirements for companies related to risk management and internal control beyond monitoring accounting systems for preparing financial statements, where are they?
In the law – Sarbanes-Oxley Act, together with associated SEC and PCAOB rules.
2. What is the scope? • **Subject matter / types of risk?**
Two sections of the Act are relevant: • s302 covers disclosure controls i.e. those over disclosures in SEC filings, which will include financial reporting controls and compliance with certain other sections of Securities Acts and SEC rules. • s404 covers financial reporting controls.
• **Types of activities?**
s302 requires CEOs and CFOs to certify on a quarterly (for domestic registrants) or annual (foreign private issuers) basis their responsibility for disclosure controls which they have designed to ensure that material information is known to them and evaluated for effectiveness, presenting their conclusions in the filing with details of significant changes and disclosing to the audit committee and auditors any significant deficiencies / fraudulent acts. s404 requires management to state in their annual report their responsibility for establishing and maintaining adequate controls over financial reporting together with an assessment of effectiveness (and the framework used in accordance with that framework).
3. Is there a framework, and if so which one?
s302 makes no reference to a framework. The SEC rule on s404 specifies an "appropriate" framework, indicating COSO, CoCo and Turnbull are appropriate. However, the auditing standard suggests that COSO is currently the only "auditable" framework.
4. What enforcement and specific legal or similar sanctions are there?
Failure to comply with s302 / s404 is subject to enforcement action by the SEC. There is no regulatory intervention if inadequate controls are reported.
5. What is the involvement of the external auditors, if any, beyond public reporting obligations on financial statements?
Section 404 of the Sarbanes-Oxley Act: PCAOB Auditing Standard No. 2 requires auditors to carry out an integrated audit of internal control with the audit of the financial statements and to express an opinion as to whether (a) management's assessment is fairly stated and (b) the company has maintained effective internal control over financial reporting as of a specified date.

The standard sets out a detailed process for auditors to follow. They are required to look at the design of controls, determine which controls are significant, evaluate design and operating effectiveness and conclude as to whether there are any significant deficiencies or material weaknesses.

The guidance in the standard is very prescriptive in terms of the extent to which management's own work can be used, issues that automatically imply significant weaknesses and the extent of testing required. The guidance also in effect sets rules for management as it sets out situations which would require automatic qualification by the auditor.

Section 302 of the Sarbanes-Oxley Act:
No external auditor's involvement required.

6. Are national changes under consideration?

New 'frequently asked questions' are being issued by the SEC and PCAOB every few months to interpret the standards. It is expected that, having got the first reporting season out of the way for domestic registrants, some questions will be issued relating to foreign private issuers who are subject to delayed implementation of the requirements of s404.

The SEC has asked COSO to produce a guide by July 2005 on implementing COSO for smaller entities (specified as those having a market capitalisation of less than $200m).