CBI
THE VOICE OF BUSINESS
40 YEARS

CBI response to March 2005 Federation of European Accountants' discussion paper on internal control & risk management

5 October 2005

Introduction

We welcome FEE's consultation on the question of Europe's approach to risk management and internal control.

We respond to the consultation questions but have also set out our members' general comments on the UK approach to the question of risk management and internal control and the differences which they see with the US approach.

Essentially we believe that the UK system works well and is supported by our members. We support the recent review of the UK's Turnbull Guidance led by Douglas Flint, which has led to a few suggestions for change, but which has also recognised that overall the UK approach has worked well.

The UK has a long tradition of corporate governance, based on a requirement in the Listing Rules for listed companies to "comply or explain" against the UK's Combined Code of Corporate Governance (the UK Code) rather than prescriptive legislation. Companies' experience of the UK Code has been of regular refinement of the detail in order to keep up to date, whilst maintaining simple, easily understandable content which is focussed on high level principles rather than overly detailed rules.

By contrast, we recently asked our members for their views on Sarbanes-Oxley in advance of the SEC Roundtable in April 2005. A major concern there is the approach of having detailed implementing rules as opposed to a principles-based approach. A key danger in corporate collapses is the potential for executive manipulation of the accounts, in which the tone at top not detailed rules for subordinates is of the most importance.

Our members therefore strongly support the existing UK concise, high level approach, in sharp contrast to their US experience with the implementation of the Sarbanes-Oxley Act, and its very detailed and costly approach.

Susannah Haan – Legal Adviser – Company Affairs
DL: 020 7395 8047 **DF:** 020 7836 1114 **E:** Susannah.Haan@cbi.org.uk

CBI Centre Point 103 New Oxford Street London WC1A 1DU
T: +44 (0)20 7379 7400 **F:** +44 (0)20 7240 1578 **W:** www.cbi.org.uk

Key differences between Turnbull and Sarbanes-Oxley

The fundamental difference between the Turnbull guidance and the Sarbanes-Oxley Act are in both approach and scope. The view of CBI members is that Turnbull makes companies think holistically about risk and controls, while Sarbanes-Oxley makes companies think about compliance within the narrower confines of financial reporting controls.

The way in which the Sarbanes-Oxley Act has been implemented requires huge amounts of detail in a narrower area and encourages a tick-box mentality. In addition, the perception among employees that the work is not really related to the real risks facing the company makes for a dispiriting environment in which to work, creates a culture of contempt for "stupid" rules and therefore breeds disregard for compliance with the spirit of the law.

By contrast, Turnbull focuses the attention of boards on the major and material risks relevant to their business, on their own responsibility for processes and on management's responsibility for implementation. The Turnbull Guidelines have changed the control and governance culture within companies but without the major additional costs that US listed companies are faced with in complying with Sarbanes-Oxley.

An important difference between the UK and US approach concerns the length and amount of detail – the Turnbull Guidelines, which provide guidance for boards of directors on the interpretation and implementation of the UK Code is only 10 pages long. While the requirements in the Sarbanes-Oxley Act themselves are not very long, the SEC has issued explanatory rules and the PCAOB has also issued its own rules, following which the audit firms have all written their own interpretation of how to deal with the issues.

This means that companies in the US need to be familiar with hundreds of pages of rules and guidance. It also ensures that senior management and members of the audit committee are unlikely to be familiar with much of the detail, unlike the Turnbull Guidelines, which has proved to be very helpful both to audit committees whose members are after all part time, and to others within the organisation.

Conclusion

Europe should focus on implementation of the 4th, 7th and 8th company law directives in a sensible, principles-based way and should not seek to legislate further nor to add detailed implementing rules to legislation. Ever more detailed guidance only gets in the way of taking a sensible approach and using judgement.

What the market really wants is to see discussions taking place between companies and investors with investors telling companies direct what they would find most useful – not ever more guidance which is audit firm or regulator led. This cannot be done by legislation but by dialogue. We do not therefore see a role for future European action other than exchange of best practice, which will be important.

There is currently severe legislative fatigue among our member companies. What companies really want to see in reporting terms is a pause to enable them to digest the Financial Services Action Plan, the Sarbanes-Oxley Act, the introduction of IFRS and the short term measures under the Company Law and Corporate Governance Action Plan.

The medium and long-term measures of the latter need to be revised as against better regulation principles and unnecessary measures should be dropped. The short-term measures should also be reviewed to see whether these are achieving their aims or whether there are any unintended consequences such that changes are needed.

In all of this, the focus should be on the companies themselves and what the investors find most useful. The UK experience has shown that a high level, principles-based approach has won support from both companies and investors. We hope that Europe will continue to choose this rather than the US approach as its model for the future.

Responses to FEE questions

1. **Do you agree with FEE that there is a need to promote discussion and evidence gathering to encourage co-ordination and convergence of the development of risk management and internal control at EU level? If not, please explain. (Section 2.4)**

   We agree that it would be helpful to promote discussion and evidence gathering in different EU member states in order to encourage sharing of best practice. However, it is important that the views of companies and investors are also taken into account and given more precedence, as well as those of the audit firms.

   Some of our members have complained that their experience of auditors in some member states, notably Germany and Austria, has been unduly rules based and it would be helpful if European discussions could lead them to adopt a more risk-based approach.

   We would have concerns about EU convergence, however, if this led in the direction that the US has taken. We would also disagree that discussion and evidence gathering should lead to action by the EU institutions. Instead, we would hope to see best practice spread across Europe as a matter of market practice. While FEE may have a role to play in this, it should be as representative of the audit firms in touch with the firms' clients rather than as a branch of any regulators.

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)**

   We agree that public policy should focus on listed entities rather than private companies and do not see any pressing need to look wider. However, there needs to be a distinction between the different types of listed companies – what may be appropriate to a company with listed shares may not be appropriate to other listed entities.

   We also believe that public policy in the EU should be focussed on encouraging the development of high level principles rather than detailed rules. The UK's Turnbull Guidance, which has been recognised by the SEC and is highly regarded, is principles-based. It is also short and readable.

   Our members are less supportive of the need for action at EU level, however, which goes beyond discussion to regulation. Companies are currently suffering from regulatory fatigue and have no desire for additional proposals in this area. While we agree that there is a potential risk that national initiatives may work against the integration of capital markets in Europe, this is not a certainty. Experience of corporate governance generally has shown a move towards convergence on the key issues. We would therefore expect best practice within Europe to converge and we would agree that the European Corporate Governance Forum could play a useful role here in discussing the different initiatives. We would not, however, support an assumption that such discussions should lead to further regulation.

   We would agree with FEE that any future proposals should be subject to evidence about the likely costs and benefits.

We note FEE's comment that "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".

If we want to encourage individuals to use their own judgement, we need to ensure that there is recognition that corporate failures will happen. No system of regulation can ever be foolproof against human and business failure.

The mere fact of such failure is not necessarily proof that more regulation is required. If, for example, the failures are in part because existing rules have been ignored, it seems unlikely that any additional regulations would have been taken into account. It is also possible to have failures through misjudgement. What may appear clear with the benefit of hindsight is often only one option among several at the time. While this may in some cases lead to failure, it is not necessarily the fault of particular individuals. The perception among many CBI members is that there is a trend towards making individuals carry the blame inappropriately. This can discourage individuals from taking up board positions in the first place. We are aware of several member companies which have had difficulty in recruiting individuals onto their boards. Public policy needs to take into account the fact that there is a balance to be struck between responsibility and risk, beyond which individuals may simply choose not to serve on company boards.

Modern global businesses are complex. The burden on individual directors in an increasingly competitive international marketplace is growing. Nevertheless the role of the non-executive directors in the UK's unitary board system (who are after all part-time) is not to second guess the management. Instead the members of the unitary board share responsibility for the stewardship of the business. They cannot be expected to know every single detail of all aspects of the business. Not should they be expected to do the job of the finance department. Their role is to set the tone and the policies and it is for management to take the decisions on the detail.

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)

We strongly agree.

We are not supportive of additional regulation in the area of internal controls; instead we strongly support the approach recently taken by the Turnbull Review Group in looking at internal controls in the UK, which decided that the system in the UK essentially works well and does not need to be rewritten but only tweaked.

We support the use of codes and the "comply or explain" approach as a better alternative to regulation. The UK experience has shown that this approach can work extremely effectively and is supported by companies and investors alike.

It is important that the regulatory environment should not create a disincentive for people to join the boards of listed companies.

We also agree that liability needs to be reasonable – in some cases, this may mean that there need to be safe harbours for directors but the key for ensuring that fear of liability does not prevent the exercise of judgement is to ensure that the directors' judgement cannot be overturned later with the benefit of hindsight. This also means that criminal liability should be limited to cases of fraud where intent is involved rather than used for mistakes.

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?

No.

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

The matrix is reasonably clear. However, it does seem to be something of a typical adviser's approach with presentationally pleasing diagrams, whereas the key question for the board is: is the board happy with the approach being taken? Does the level of risk feel right? That is the matter for the board's judgement.

The danger of the FEE model is that the focus is on whether there are enough ticks in the boxes. It looks a little too much like encouragement for a rules-based approach and as such seems to follow the US approach too closely. It also seems to suggest that companies should aim to be able to tick all the boxes at some stage. We would question this approach.

We much prefer the UK's Turnbull guidance, which sets out key questions for the board and which our members have found to be extremely useful in improving risk management. We set out below some comments on our members' experience of the UK model.

UK experience of the Turnbull Guidance

When the Turnbull guidance was first introduced, many companies felt they had to establish risk registers and other fairly bureaucratic systems in order to demonstrate to shareholders and regulators that they had appropriate controls and risk management policies in place. There was a lot of activity from consultants and promoters of IT software. However, the focus now is on board decisions rather than IT systems and on common sense and real risks rather than "tick the box" lists. There were initially some compliance costs, but these were insignificant when compared with our members' US experience, where the costs have been huge.

Many originally sceptical CBI members have come to realise that the Turnbull guidance is very useful. (As a matter of detail, while the Sarbanes-Oxley Act focuses on financial reporting risk, the Turnbull guidance applies to all risks and controls, not just those related to financial reporting).

The main reasons for this are that:

- the guidance does not lay down lots of detailed, prescriptive rules, but has set high level principles which are worth rereading and which have positively changed attitudes and the way in which businesses are run

- it is regularly reviewed by senior business people (users of the guidance not advisers or regulators) respected by their peers and is updated to ensure that it continues to reflect changing business needs

- it is relatively short and clearly written, which means that it is accessible to members of the board, managers, auditors and employees, rather than requiring the assistance in interpretation of lawyers and accountants. This helps to ensure that the responsibility for risk management rests where it should – with the board and management – with the board's focus on major and material risks, on their own responsibility for processes and on management's responsibility for implementation

- the purpose of the guidance is clearly stated as being to establish a sound system of internal control, which should be treated as part of the normal management and governance processes, rather than as a separate regulatory exercise. This has been important in embedding proper risk management within companies' culture. The guidance also clearly sets out the fact that internal control systems may reduce, but cannot eliminate, errors, nor provide absolute assurance against fraud or other factors, again enabling the board to emphasise the need to encourage vigilance rather than merely comply with the law.

We would be happy to provide further information on any of the points above.

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?

No. We do not see any such need and we agree with the concerns set out by FEE. There are already three well established frameworks accepted by the SEC – COSO, COCO, and the Turnbull Guidelines. There are therefore already several market models which work.

If one were nevertheless to be developed, we would see any framework best developed by market practitioners - at all costs it should be kept out of the hands of financial regulators and should be led by companies and shareholders with audit firm input. Otherwise it would be in danger of turning into the bureaucractic nightmare which exists in the US. It would be essential for any such framework to be kept short – the Turnbull Guidelines are only 10 pages long and yet sum up all the essential issues.

We note that section 404 of the Sarbanes-Oxley Act is only a paragraph. However, the Sarbanes-Oxley Act gave implementing powers to the SEC and PCAOB to create additional, more detailed rules. The guidance and rules on Sarbanes-Oxley run to hundreds of pages, which makes it difficult to distinguish the essential from the unimportant and makes it inaccessible to many. Compliance with these rules requires huge amounts of detailed work and encourages a tick-box mentality, which is unlikely to prevent future corporate failures.

We repeat that we do not see the need for any action from a UK point of view. Companies feel that the Turnbull guidance works well and have no desire to see additional European guidance / regulation. There is concern based on past experience that a "framework" on risk management and internal control would not be that at all but would rather be very detailed and prescriptive.

Our members' experience in the US with the Sarbanes-Oxley Act has highlighted the following dangers:

- Contradictory and inconsistent PCAOB audit standards and guidance implementing the Sarbanes-Oxley Act, especially AS No. 2. There is very little commercial perspective or feel for balance as would come from a more principles-based approach.

- Given the manner in which the PCAOB auditing standards are written, the external auditors feel that they have been made judge, jury and executioner of the financial statements whereas it should be the job of management to ensure that the financial statements are properly made. The auditors should only be asked to attest to whether the company has followed the auditing standards, not give opinions as to internal control effectiveness and second guess management's conclusions. Given their position outside the company, the auditors are in a position to review the facts but not to pass judgement as to what material weaknesses are. As a result, the external auditors tend to take a very conservative interpretation when applying the standards in practice, with the huge consequences for compliance costs that we see now.

- Overly detailed implementation requirements for testing of the internal controls (with apparently no weaknesses in tests being tolerated, however immaterial to the enterprise overall). The detailed rules have led to focus on minutiae, leading many companies to work from the bottom up from detailed lists of risks rather than top down by looking at the key risks to the business and working back to deal with those key risks first. This stands in contrast to our members' experiences in the UK, where companies are required to have systems in place that have to be reported on, but which are proportional to the company and the risks which it faces. The board has the responsibility of making sure that the procedures are in place to allow for proper risk management but is not expected to micromanage.

- Documentation – the level of documentation required is unrealistic and costly. Even if a company has effective controls in place, it may not have the resources to produce the documentation required to prove this to the satisfaction of the auditors. There is also duplication of work by management and the audit firms.

- Costs are not felt to be proportional to the risk. Companies have already invested significant amounts of money in complying with section 404 requirements but do not feel that the current level of cost or resource is sustainable. In the ordinary course of business, companies invest in IT systems, reorganise their operations and personnel and acquire/divest assets. Each of these activities will require internal controls to be modified and retested and yet should not necessarily be key concerns.

- Delay in adding shareholder value - Sarbanes-Oxley as implemented is causing companies to delay other commercial projects which would add shareholder value, particularly on the IT side. This is due to both the lack of available resources (in terms of management time and money) and fear of the impact on internal controls. This is a real cost as it threatens the business' ability to grow and adapt and potentially damages shareholder value. This is related to the issue of:

- Regulation versus ownership – companies' disclosure is being driven by the PCAOB, by the concerns of the audit firms to avoid litigation and by a culture

of compliance with rules rather than by focussing on real risks and disclosure of most value to shareholders as owners of the business.

- Competitive disadvantage - the Sarbanes-Oxley Act puts companies listed in the US markets at a competitive disadvantage compared with their peers that have not chosen to have their securities listed in the US. This ultimately harms the long-term interests of investors.

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)

We agree in principle with the disclosure by companies of their overall approach to risk management at the highest level. However, there is a need to ensure that any disclosure principles are not too specific or prescriptive, since this would impact on individual company's appetites for risk and therefore risk management style.

We agree that disclosure of information needs to be useful to shareholders and that the benefits should outweigh the costs. However, the annual report and accounts for many companies is now several hundred pages and both the companies and the investors complain that much of the information is of little interest to them. It would appear that the current situation is already one where the costs of providing existing information outweigh the benefits.

It may in some cases be necessary to provide safe harbours in order to encourage the provision of useful information without fears of liability.

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

The problem is that any conclusion that the internal controls are effective is likely to be used against the company in litigation later if something does go wrong. Companies are therefore extremely reluctant to make such statements. We support the conclusions of the Turnbull Review Group, which decided against recommending such a requirement.

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)

From the UK point of view there is already such a requirement so it would add nothing of benefit for UK companies.

If what is being proposed is similar to sections 221(1) and 237(1-3) of the UK Companies Act 1985, however, we would not disagree with the content. Nevertheless, we would not support more extensive requirements than exist in the UK.

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)

No. The important thing is that companies should be allowed to develop their own criteria and should explain which criteria they use.

If there is felt to be a need for some criteria, perhaps some existing frameworks such as the UK's Turnbull guidance could be endorsed – we would note that it is now a recognised SEC framework – if it were to be endorsed perhaps this should be by private bodies such as FEE in the first instance. There may be other such national frameworks but we can only speak for the UK. But we believe that the market should be allowed the chance to develop its own criteria and believe that there is no need for these to be developed by the European Commission.

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

Regulatory requirements should be kept to a minimum. They should be restricted to a high level requirement for companies to have systems in place but should not go the US route of prescribing in detail what those systems should be. That is costly and unnecessary.

Real improvements in risk management and internal control are driven by ownership by the company. The danger is that regulatory requirements become a distraction from real improvements and lead instead to a focus on compliance with rules.

We agree with 5.5.3 that it can be difficult to communicate meaningfully but believe that more dialogue between companies and shareholders with shareholders being clear to companies what information they would find most useful would assist with more meaningful disclosure than regulation. We also believe that the increasing volume of information required to be disclosed in the annual report makes it more difficult for companies to communicate clearly.

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?**

We agree with the identification of the issues but disagree that it would be desirable for regulators to develop high level criteria for disclosure.

We also disagree that statements of effectiveness provide a strong incentive to make better disclosures of overall process and the management of specific risks.

The recent UK consultation on the Turnbull guidance has shown that both companies and investors are sceptical of the benefits. The experience of the UK has been that this leads to concerns about liability and thus to boilerplate disclosure. Concerns about liability should the statement say that the controls are effective inevitably lead to caveats which reduce its usefulness.

We agree that it will be important to learn from experience.

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

We are not convinced that Europe should aim to achieve reporting on all types of risk set out in the table and believe that this could give a misleading impression of benefits. See comments elsewhere on effectiveness.

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).

Within the UK the combination of a comprehensive report on corporate governance by the company management, combined with a report on the audited financial statements by the independent auditors, is considered to provide adequate assurance to investors, who also have the opportunity to challenge any issue on the running of the business, at the Annual General Meeting.

The work of the Commission on shareholder rights to remove barriers to cross-border voting should assist EU investors to raise issues at the General Meeting, thus improving corporate governance.

Investors also have the opportunity to raise concerns with the company during the course of the year and most companies would very much welcome direct feedback from their investors on what information they would find most useful.

We therefore consider that the best way of providing assurance is via dialogue between the company and its investors rather than via the audit itself, which should be limited to objectively verifiable information.

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)

No. We agree with FEE that auditors should not be involved in areas that are not objectively verifiable.

We do not agree with the US PCAOB approach of the integrated financial statement audit which requires a double opinion on both internal control and the financial statements.

We have seen that the approach being taken by many audit firms to Sarbanes-Oxley is very rules oriented, especially in Germany and Austria. Our corporate members' experience (which includes German companies) is that the profession in some countries is less able to take a risk oriented view, with greater costs to companies with extensive operations in those countries.

Auditors are naturally risk averse (which is what you want to ensure that management does not overinflate earnings) but this means that they are not naturally good at managing risk and are not happy being placed in this position. The audit firms tell us that they feel that the current US requirements are detrimental to quality and make discussions with management more defensive. The companies tell us that the new role of the auditors in the US creates a less open atmosphere and chills communication between the audit committee and the auditors, for fear of repercussions if matters are raised with the auditors at too early a stage and the auditors then overreact.

In the UK, internal control has been part of the Combined Code. UK auditors do some limited work on the statement on the Code but this is limited to a

consistency check. The purpose of this is to provide investors with reassurance that there is a process but not to provide any comment on the content.

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)

The key priority for companies is to be allowed a period of calm in order to be able to digest the huge amounts of work involved in IFRS, the implementation of the Financial Services Action Plan, the Sarbanes-Oxley Act, the 4th, 7th and 8th company law directives and other national initiatives over the past few years.

New proposals for regulation are a distraction from this and prevent the latest changes from having the chance to become embedded in the company's culture.

The issue of liability for both auditors and directors may need to be considered.

16. Do you have any other comments on this discussion paper not covered by the specific questions reproduced above?

Directors & Officers' insurance

One issue which has not received a lot of attention to date is the impact on Directors & Officers' insurance. Views on premia may change quite radically as the insurers become nervous about compliance. Some companies may find that they cannot obtain such insurance for their directors and officers. The risk of this will be higher for entrepreneurial companies, which could lead to a two-tier system.

There is also the issue of recruitment. It is getting more difficult to recruit non-executive directors onto boards. To the extent that this relates to a better understanding of their personal risk, this is not necessarily bad. However, the perception clearly is that the risks related to sitting on the board of a company listed in the US are too high.

If regulation is causing difficulties for companies in recruitment, then that regulation may need to be reconsidered. We also need to look for any potential unintended consequences – if those companies that are in most need of the best people cannot recruit, what will be the effects on the market?

Comments on the Sarbanes-Oxley Act and its interaction with IFRS

The Turnbull guidance and the Sarbanes-Oxley approach are viewed by CBI members as chalk and cheese. The Sarbanes-Oxley Act focusses on financial reporting controls, whereas the Turnbull guidance applies to all aspects of internal control. The auditing standards under the Sarbanes-Oxley Act are mainly intended to regulate the audit profession but also have considerable impact on companies.

Section 404 of the Sarbanes-Oxley Act requires a statement on effectiveness in the annual report, with a requirement for the audit firm to attest to this. However, the Sarbanes-Oxley Act also gave implementing powers to the PCAOB to create additional, more detailed rules. The specific rules created under the Sarbanes-Oxley Act by the PCAOB have only exacerbated the difficulties. The PCAOB's definition of material weakness refers to "anything other than a remote likelihood" of a restatement occurring. Naturally the company's advisers are reluctant to state that most risks are only a remote likelihood. This means that companies are having to

disclose all manner of "weaknesses" which are in reality not perceived as being closely related to the real risks facing the business.

The PCAOB approach is a significant concern with the introduction of International Financial Reporting Standards. The more fair value based standards of IFRS mean that many reported figures will be more liable to volatility – hence boards will be even less likely to feel comfortable with public statements on effectiveness and even more inclined to be concerned about legal liability.

Comments on the 8th company law directive on statutory audit

It will be important for auditors, companies and investors to work together to ensure that implementation in the Member States of the 8th company law directive with its reference to material weaknesses in Article 39 is clearly directed only at issues arising directly from the statutory audit and that the definition of material weakness is something which is genuinely material i.e. which could impact on the financial position of the company, rather than the PCAOB definition.

It will also be important to avoid implementation which may lead to a focus on compliance rather than the objective of improving risk management.

CBI additional comments on FEE Proposals (pages 6-7)

- **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)**

We strongly agree. The focus should be on risk management not risk avoidance. We also strongly believe that the use of judgement is key and that risk-taking is a necessary part of running businesses.

The best way to ensure that companies can exercise judgement is to encourage best practice rather than prescriptive rules and to ensure that high level principles applicable to all are followed, rather than detailed rules which will need to be adapted and expanded to fit many different circumstances.

We agree that the emphasis should be on learning from experience so that the circumstances most relevant to the individual company can be taken into account rather than have a prescriptive "one size fits all" approach for all companies regardless of size and complexity.

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

We agree that the focus should be on principles. Our members do not believe that detailed rules would prevent another Enron, because other factors such as the tone from the top are equally important. However, such rules do divert management time away from value adding projects, thus hurting investors.

We do not believe that principles should be developed by the regulatory authorities but rather by market participants. We are not supportive of additional EU regulatory developments.

The UK approach has been to focus on accountability, transparency and disclosure rather than prescriptive regulation and to recognise that much of corporate governance is less suitable for legislation but rather depends on the integrity of the individuals involved and on dialogue between the board and its shareholders. The UK Combined Code acknowledges the freedom of the board to manage the business as it sees fit but to account to it shareholders for its stewardship in the annual report and accounts. This is in line with the principle of subsidiarity.

We note that the recent SEC statement has urged companies to move to a more principles-based approach. However, it is highly questionable whether the implementing rules and regulatory guidance in the US will assist companies to do this. In particular, the PCAOB implementation of Sarbanes-Oxley with its definition of material weakness as "anything other than a remote likelihood" of a restatement occurring is felt to be particularly unhelpful. Dealing with risks based on the basis of a remote likelihood not only imposes huge costs but also makes this a "nitpicking" process, the very nature of which seems to get in the way of any potential success for internal control reporting as a useful management and shareholder tool.

- **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)**

We could agree to this, provided that what is being proposed is along similar lines to the current UK requirement but goes no further than that.

- **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)**

We agree. We hope that the measures in these directives will not involve significant change for UK companies although we appreciate that there will be more change for companies incorporated in other EU member states.

We believe that the most effective change is that of culture, which takes time to be embedded within the company.

- **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)**

The UK's Turnbull guidance makes specific reference to the need for risk management to take place as part of the company's normal management and governance processes, rather than as a separate exercise undertaken to meet regulatory requirements.

While there are some high level criteria, these are kept short and simple. We assume that the 4th and 7th directives rely upon high level provisions in national codes such as the Turnbull guidance, which we support. We do not support regulatory development of yet more criteria.

- **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)**

We agree that an evolutionary path is preferable and ultimately more likely to be effective. But we see the main challenges as cultural not legislative or regulatory.

- **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)**

We agree. The most effective way of bringing about meaningful disclosure is genuine demand from shareholders. The UK experience of the "comply or explain" regime has been that the dialogue between companies and shareholders has led to far greater understanding on both sides and has mostly worked well.

What is more important than detailed rules is to ensure the appropriate exercise of power. In this respect, we support action by the EU to give shareholders greater powers to vote cross-border. By contrast, the fundamentals of US corporate governance are still perceived by the outside world to consist of weak shareholder rights, meaning a lack of investor leverage to prevent corporate greed. The US legislative approach should be judged as against its own particular background.

An example of the effectiveness of rating agencies is Moody's analysis of companies' disclosure under section 404 of the Sarbanes-Oxley Act, which was far more pragmatic than the PCAOB approach. The latter forced companies to spend time and effort on areas which are really not that important and do not present a real risk of failures in financial reporting. Moody's approach is perceived as more relevant and thus more likely to influence corporate policy than the regulatory approach. However, companies are most interested in the views of their direct shareholders and these are seen as the most effective mechanism.

- **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)**

We agree. Companies do not wish to make a statement on effectiveness and the recent UK consultation on the Turnbull guidance has shown that investors are also sceptical of the benefits. The experience of the UK has been that this leads to concerns about liability and thus to boilerplate disclosure.

The US statement of effectiveness is perceived to underlie a key psychological difference between the Turnbull and Sarbanes-Oxley approaches. Under Turnbull, the perception is that companies should have an incentive to publish changes made since these represent positive news, as companies which have made changes have presumably improved their risk management. The Sarbanes-Oxley approach, however, with its requirement for a statement of effectiveness, is perceived to lead to fears of litigation. This could potentially create negative management incentives and encourage a culture of burying bad news since companies know they will be penalised for disclosure. Disclosure of effectiveness is thus viewed by companies as a "no win" situation.

- **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)**

We agree. The auditors are only advisers to the company; the primary responsibility rests with the company itself.

- **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)**

We disagree. This sounds like support for the PCAOB model led by the regulator and the audit firms rather than the company / shareholder led approach, which we support.

If auditors do not wish their responsibilities to exceed those charged with governance as above, they must also accept that they have a key role in advising / auditing but not in making business decisions. There is a danger that some detailed work by audit firms / regulators could take responsibility away from the companies – and hence put more liability on the audit firms.

- **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)**

We agree - provided that what is being stated is referring to the auditors being able to conclude this as part of their normal audit work. We would disagree if this is suggesting a separate opinion on internal control as PCAOB Standard No. 2 does.

There is some danger in an over-emphasis on record-keeping as exemplified by the Sarbanes-Oxley approach. Many of our member companies have expressed their concern that they felt that they had systems of internal control in place prior to Sarbanes-Oxley but not the pieces of paper to prove this. Too much emphasis on procedure creates irritation and undermines the relationship between companies and their auditors.

There are some requirements in UK law which have worked well but these are more limited than the US approach.

- **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)**

We do not recommend the take up of the US PCAOB approach in Europe as a global standard. On the contrary, we believe that Europe should take a different and we believe more effective approach.

The development of any standards therefore needs great care. We would reiterate our earlier points about the usefulness of the high level UK approach versus irritation at the huge amount of unnecessary detail in the US.

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

We agree. We support reform of auditor liability in the UK but believe that liability should remain as a member state issue. However, see also our responses to questions 13-14.

About the CBI

The CBI's members, which decide all policy positions, include approximately:

- 80 of the FTSE 100
- 50 US listed companies
- major UK investors
- some 200,000 small and medium-size firms
- more than 20,000 manufacturers
- over 150 sectoral associations
- the Big Four audit firms plus mid-tier audit firms

The CBI is the UK's leading business organisation, speaking for some 240,000 businesses that together employ around a third of the UK's private sector workforce.

With offices in Washington as well as across the UK and in Brussels, the CBI co-ordinates British business representation around the world.