National Office

Grant Thornton UK LLP
Chartered Accountants
UK member of
Grant Thornton International

Our Ref CSSD/SM/NJJ

Director of Practice Regulation
Federation des experts Comptables Europeens
Avenue d'Auderghem 22-28
B - 1040 Brussels
BELGIUM

For the attention of Hilde Blomme

27 July 2005

Dear Sirs

RISK MANAGEMENT AND INTERNAL CONTROL IN THE EU DISCUSSION PAPER

Most of the key proposals in this paper are written with a view to minimising bad business decisions. The paper deals with the positive side of risk management in helping those boards who wish to manage risk - the paper does not address how to prevent someone senior in the organisation from ignoring or overriding those procedures. It is a widely held misconception that effective risk management would eliminate financial scandals. Whilst it is true that certain terminal collapses have been hastened by poor business decisions many scandals arise where senior management have circumvented the system of controls that they themselves have been charged with designing and implementing, for example by omission of certain transactions from accounting records.

By its very nature a system of internal control has loopholes - a system is predictable. At best, a sound system of internal control makes it easier to say to directors when things go wrong that they have perpetrated a fraud or that they have knowingly ignored certain safeguards and removes the defence of "I did not know I was supposed to do that". In our view it is incumbent on regulators to address this misconception. A good start might be for regulators to stop saying "Recent corporate scandals drive improvements in corporate governance".

Principles must underpin any regulatory developments.

A basic starting point is that companies maintain accounting records that support information included in published financial statements and that this requirement be enshrined in company law.

We strongly agree that the duties incumbent on external auditors with regard to risk management and internal control cannot exceed the responsibilities of those charged with

Grant Thornton House
Melton Street
London NW1 2EP
T +44 (0)20 7383 5100
F +44 (0)20 7383 4715
DX 2100 EUSTON
www.grant-thornton.co.uk

corporate governance. Primary responsibility for implementing and maintaining effective control systems must rest with the directors; the auditors' role must be that of monitoring and reporting.

Legislators must be careful to strike the appropriate balance between the benefits to shareholders of new legislation combined with codes of practice and the costs of compliance that will imposed on the company.

We strongly agree that any new rules on risk management and internal control in the EU should be mandatory for listed companies only.

If you require clarification on any of the issues raised please contact my colleague Nick Jeffrey (*Direct T: 0870 991 2787; Direct F: 0870 991 2787; E: nick.jeffrey@gtuk.com*)

Yours faithfully

Steve Maslin
Head of Assurance Services, partner
For Grant Thornton UK LLP

QUESTIONS FOR COMMENTATORS

INVITATION TO COMMENT

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

2: THE CASE FOR RISK MANAGEMENT AND INTERNAL CONTROL

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

Yes. The EC could help to raise the minimum level of risk management and internal control across the EU by implementing a framework of common principles.

However the evidence gathering phase might usefully focus on the cause of financial scandals. At present many commentators assume that financial scandals means that better corporate governance is needed but evidence might show that even improved internal controls would not have prevented the scandals we have seen.

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.*

Yes - EU public policy should focus on listed companies and their shareholders. If the scope were any wider it would be unnecessarily onerous on those companies that are not public interest entities.

No - we do not believe there is a pressing need to deal with issues of a wider range of entities or stakeholders.

3: OVERRIDING PRINCIPLES

3 Do you agree with FEE that the case for introducing any regulation related to risk management and internal control should have regard to: the business case for risk management; the advantages of principles-based requirements; the distinctive features of listed companies; the primacy of those charged with governance; and reasonable liability? If not, please provide details.

Yes. Any regulation should be in the style of "comply or explain" by reference to a Code of Practice. Any legislation should be a bare minimum. This will allow faster and easier development of good practice in the field.

4 *Are there overriding principles additional to those identified by FEE in Section 3.1 to 3.5 that are relevant to risk management and internal control? If so, please explain.*

Reference to fraud would be useful - any system of internal control would be expected to include reasonable steps to prevent and detect fraud but cannot be expected to eliminate fraud or other irregularities.

4: ISSUES TO BE ADDRESSED

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 useful in giving a snapshot of how controls can be used to address identified risks. The matrix does not easily identify the relative impact of individual risks, and does not readily lend itself to the dynamic nature of a system of internal control which must evolve as the nature and size of the business changes.

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 believe that there is a need to develop an EU framework for risk management and control. There are existing frameworks, such as the Turnbull Guidance issued by the UK's Financial Reporting Council and the guidance issued by COSO, which could be referred to as "acceptable for the purposes of the Regulation".

7 *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?*

Shareholders assume that quality management will implement a system of internal control and risk management that is proportionate and tailored to the entity's business. At most any EU regulation should stipulate only that the annual report should outline the overall process of risk management and internal control. We believe that the final three disclosure principles (performance reported against stated criteria; disclosure of measures to address issues or problems; disclosures should link risk to business strategy) are desirable and should be encouraged but that they should not be compulsory. It is for directors to decide, after consulting their own shareholders, what disclosures should be made.

5: REGULATORY OPTIONS AND PROPOSALS

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?*

Yes - this is a vital building block for sound internal financial control.

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?

No - there are already frameworks in use within the EU which could form the basis for meaningful disclosures such as the Turnbull Guidance issued by the UK's Financial Reporting Council or the guidance issued by COSO. It might be considered unfair to recommend or even impose UK guidance (which many consider to lead the world) on emerging capital markets around the EU. Meaningful descriptions should be "aspirational" or good practice rather than "mandatory". Companies will soon improve disclosures if they find that their share price is suffering because of limited or boilerplate disclosures on risks and internal controls.

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

Regulatory requirements should be kept to a minimum high-level disclosure requirement at most. Developing best practice is the most efficient way for long-lasting improvements to be made.

It is perhaps not for inclusion in legislation, but any code of practice should encourage shareholders, particularly institutional shareholders, to engage in constructive dialogue with their investee companies. Shareholders have a vital role to play in shaping how companies tell shareholders what they do and why. Ultimately shareholders might have to disinvest should they be dissatisfied with how the company is run.

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?*

Shareholders take it as read that management will identify risks and implement appropriate procedures to manage those risks. Section 2 is the important element to them - institutional shareholders take it for granted that quality management will seek to manage risk. Sections 1, 3, and 4 (disclosures of overall process, disclosures of management of specific risks and disclosure of effectiveness conclusions) are not so important to shareholders as knowing that a thorough process takes place. Having said that, meaningful disclosures on specific risks and steps taken to mitigate those risks can bring to life disclosures that otherwise might appear boilerplate.

We do not believe that directors should be required to make a statement as to the effectiveness of the system of internal control.

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

More progressive companies will try to make disclosures about specific risks and controls to mitigate those risks. Specific disclosures are obviously better for shareholders than boilerplate statements but this must be optional - it must be left to directors to decide what to say and how to say it.

We do not believe that publication of "effectiveness conclusions" should be required. There are obvious issues of liability and we are not aware that there is a clear call from European shareholders for effectiveness conclusions given the extremely high costs associated with (Sarbanes Oxley) section 404 assignments in US listed companies.

6: EXTERNAL ASSURANCE

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.*

The financial statement audit gives no assurance in respect of internal controls over financial reporting - the investor is not made aware of what has happened behind the scenes in arriving at the published accounts. For example, the level and nature of audit adjustments is never published, discussions between the auditor and management of matters of judgement, appropriateness of accounting policies, weaknesses observed in internal systems and management representations remain private. We believe that as long as the audited financial statements are free from material accuracy or error then the shareholders are not overly concerned about the process of how those financial statements were generated. Internal controls over financial reporting are of more concern to shareholders where the directors publish financial information that is not subject to external scrutiny or independent assurance.

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?*

Under International Standards on Auditing (ISAs) it is already incumbent on auditors to ensure that information published alongside the audited financial statements is not inconsistent with that information or with the knowledge gained by the auditor during the course of the statutory audit. New disclosures related to risk management and internal control would also fall within the scope of ISAs in this regard.

There is also a role for the auditor to ensure that the directors have reviewed the effectiveness of the system of internal control during the year and that the directors have considered what steps to take as a result of that review.

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?*

New forms of assurance will need new forms of assurance criteria. These will need to be developed by an appropriate international body such as the IAASB.

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

No.