Chris Hodge
Corporate Governance Unit
Financial Reporting Council
Fifth Floor
Aldwych House
71-91 Aldwych
London WC2B 4HN

REVIEW OF THE EFFECTIVENESS OF THE COMBINED CODE

CALL FOR EVIDENCE – March 2009

Please find below my comments on the Combined Code. My interest in the Code stems from my involvement in risk-based internal auditing, and I am only commenting on the Board's role in relation to risk management.

I have noted my conclusions below, with the reasons behind these conclusions noted on the following pages.

Conclusions

The first principle of the Code states: *The board's role is to provide entrepreneurial leadership of the company within a framework of prudent and effective controls which enables risk to be assessed and managed.* Yet the major reason for the 'Credit Crunch' must be the failure of boards, and regulatory agencies, to fully identify the risks to which businesses were exposed; appreciate their impact and likelihood; and act to reduce them to acceptable levels. Hence the effectiveness of The Code must be questioned.

I believe the management of risks to be as important as the presentation of 'true and fair' accounts, as management can only be effective if risks are understood. My overall conclusions on the changes required to the Combined Code are therefore as follows:

- There is no main principle requiring the Board to identify, assess and record the principal risks of the company. The principle to maintain a sound system of internal control (C2) should include these procedures, but the phrase 'internal control' does not clearly convey the need for the board to ensure risks are being managed to within their acceptable levels. Many board members consider internal control to relate only to financial system controls and are considered to be the province of internal auditors. The Turnbull Guidelines are intended to clarify the relationship between internal control and risk but they are now only a footnote to the code and it is unlikely that directors would read them. I therefore suggest rewording C.2, C.2.1, and parts of C.3.2 to reflect the need to concentrate on risks. I have made suggestions for wording in the pages following.

- The audit committee chairman should report to the AGM on the result of the reviews on risk management systems and the effectiveness of the company's internal audit function, in order to ensure these reviews are properly carried out.
- The Smith and Turnbull Guidelines need to be considered part of The Code, which should include a statement that compliance with the Guidelines is expected.
- While the document should remain high-level guidance, there is a need to provide more information on the management and recording of risks, by amending the Turnbull Guidance. A company is required to keep 'proper books of account', so why not, 'proper books of risk'?
- Since the management of risks is important to the 'going concern' concept, the external auditors should confirm that the management of risks is such that it supports the continued existence of the company as a 'going concern' and that no risks which threaten the continued existence of the company have been accepted.

These conclusions should not impose additional work on any company which is observing The Code at present. They are intended to ensure that those companies who perhaps do not fully understand the requirements of The Code and Guidelines in relation to the management of risks, take appropriate action.

David Griffiths Ph.D. FCA

21 April 2009

www.internalaudit.biz

www.managing-information.org.uk/

My detailed comments on the board's role in relation to risk management

Current FRC Guidance

The FRC guidance to date on the Board's role in relation to risk management is set out below.

Combined code:

The first principle (A.1) of the Code states: *The board's role is to provide entrepreneurial leadership of the company within a framework of prudent and effective controls which enables risk to be assessed and managed.*

The Guidance on Audit Committees (Smith):

(2.2) *..that the main roles and responsibilities of the Audit Committee should include: to review the company's internal financial controls and, unless expressly addressed by a separate board risk committee composed of independent directors or by the board itself, the company's internal control and risk management systems;*

4.6 The company's management is responsible for the identification, assessment, management and monitoring of risk, for developing, operating and monitoring the system of internal control and for providing assurance to the board that it has done so. Except where the board or a risk committee is expressly responsible for reviewing the effectiveness of the internal control and risk management systems, the audit committee should receive reports from management on the effectiveness of the systems they have established and the conclusions of any testing carried out by internal and external auditors.

Revised Guidance for Directors on the Combined Code (Turnbull)

4 *A company's objectives, its internal organisation and the environment in which it operates are continually evolving and, as a result, the risks it faces are continually changing. A sound system of internal control therefore depends on a thorough and regular evaluation of the nature and extent of the risks to which the company is exposed. 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.*

15 *The board of directors is responsible for the company's system of internal control. It should set appropriate policies on internal control and seek regular assurance that will enable it to satisfy itself that the system is functioning effectively. The board must further ensure that the system of internal control is effective in managing those risks in the manner which it has approved.*

16 *In determining its policies with regard to internal control, and thereby assessing what constitutes a sound system of internal control in the particular circumstances of the company, the board's deliberations should include consideration of the following factors:*

- *the nature and extent of the risks facing the company;*
- *the extent and categories of risk which it regards as acceptable for the company to bear;*
- *the likelihood of the risks concerned materialising;*
- *the company's ability to reduce the incidence and impact on the business of risks that do materialise; and*
- *the costs of operating particular controls relative to the benefit thereby obtained in managing the related risks.*

17 It is the role of management to implement board policies on risk and control. In fulfilling its responsibilities management should identify and evaluate the risks faced by the company for consideration by the board and design, operate and monitor a suitable system of internal control which implements the policies adopted by the board.

The problems

- The code recognises the importance of the board understanding the risks which threaten the company's objectives. However, although The Code highlights the importance of managing risk in the first paragraph, it does not have a Main Principle requiring the board to identify, assess and manage risks. The most relevant main principle is C.2: *the board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets*. However:
  - Many directors, and even some auditors, associate 'internal control' only with financial systems, although C.2.1 attempts to widen the scope.
  - 'Internal control' is often seen as the province of internal audit
  - While a sound system of internal control depends on a thorough and regular evaluation of the nature and extent of the risks to which the company is exposed (Turnbull paragraph 4), internal control is only one of several systems used to manage risk, the others being to tolerate the risk, terminate the risk or transfer the risk (e.g. through insurance). Thus the emphasis of The Code should be on risk, not internal control.
  - There is confusion throughout The Code, Turnbull and Smith Guidances about the relationship between internal control and risk management. The Smith Guidance (Paragraph 4.6) refers to *the internal control and risk management systems*, despite the fact that *internal control* **is** a *risk management system*. The Code also makes this error (C.2.1). Smith also allows for a separate *board risk committee*. Thus many directors, and some auditors, believe that risk management and internal control are completely separate entities.
  - There is no attempt to define a *sound system of internal control*. There is a footnote that refers to the Turnbull Guidelines, but these are not now appendices to The Code and compliance with them is not a Code requirement. It is therefore possible that directors will not read the Turnbull Guidelines.

The use of the phrase *internal control* in C.2 limits the main principle and draws attention away from the need of the board to ensure the company's risks are being managed.

- The Code (C.3.2, second point) refers to the audit committee reviewing internal controls and risk management systems, but there is no referral to Turnbull as providing guidance for the basis of the review.
- The Code (C.3.2, third point) refers to the audit committee reviewing the effectiveness of the company's internal audit function but there is no guidance on measuring the effectiveness.
- There is no requirement in The Code for the audit committee chairman to report to the AGM on the result of the reviews on risk management systems and the effectiveness of the company's internal audit function. Thus there is no impetus to ensure these reviews have been thorough.
- The Turnbull Guidance does not contain sufficient detail on risk management. For example, it fails to provide guidance on risk appetite.
- Directors could comply with The Code but set the acceptable levels of risk so high that residual risks could threaten the continuing viability of the company.

The solutions

The underlying principles

One of the pillars of good governance is the management of risks. Thus the main aim of the board in relation to risk management must be to manage risks to acceptable levels, that is, below the Board's risk appetite. (Turnbull requires this in paragraph 16 and appendix 5 (Risk assessment): *Is there a clear understanding by management and others within the company of what risks are acceptable to the board?*

In order that the board can ensure risks are being managed to within acceptable levels, it must:

- Identify the risks faced by the company.
- Evaluate these risks with regard to their impact and likelihood, before any management is taken into account (inherent risks).
- Define a risk appetite, in terms of impact and likelihood, above which risks are considered unacceptable.
- Consider how the company's systems are reducing the risks, mainly through the operation of internal controls.
- Re-evaluate the risks with regard to their impact and likelihood, taking account of the internal controls (residual risks).
- For those residual risks above the risk appetite, consider what action is required to make them acceptable.
- Formally record these results in a risk register.

The above restates Turnbull paragraph 16 using risk management terminology, although being more prescriptive. Considering the failure of risk management in some companies, this slightly more prescriptive approach is probably justified.

Taking the above principles into account, changes to the code can be identified.

The Changes necessary to the Code

1. C.2 should read:

C.2 The management of risk

Main Principle

The board should ensure material risks are managed to within the acceptable levels it has defined, in order to safeguard shareholders' investment and the company's assets.

Code Provision

C.2.1 The board should, at least annually, identify the material risks threatening the objectives of the company, assess the impact and likelihood of these risks occurring, confirm the level of risk which the board is prepared to accept and conduct a review of the effectiveness of the company's system of internal controls, and other methods of risk management, in bringing risks to within the acceptable levels. They should report to shareholders that they have done so and that, for risks above the acceptable levels, action has been taken to bring these risks to within the levels.

2. C.3.2 should read:

C.3.2 (second and third points)

- to review the company's risk management systems (including internal controls) in order to confirm that they are sufficient to keep risks within the acceptable levels set by the board and report instances where they are not. The Turnbull Guidelines should be considered as a benchmark for this review.
- to monitor and review the effectiveness of the company's internal audit function in order to ensure that it is examining and reporting on the ability of the company's risk management systems to keep risks within the acceptable levels set by the board.

The intention of these changes is not to change the underlying principle but emphasise the importance of managing risk over the maintenance of internal controls, which is perceived as a much narrower scope. They also more clearly define the purpose

behind the reviews. (I have used the phrase ‘acceptable levels of risk’ as directors may wish to set several levels depending on the nature of business being conducted.)

3. Turnbull and Smith Guidances

The principle on internal control (and risk) is only meaningful if read in conjunction with these Guidelines. They should therefore be considered as part of The Code, which should include a statement that compliance with the guidelines is expected.

They need to be updated in order to be consistent with the amended code. In particular they need to be more prescriptive about the recording of risks and their assessment and management on a risk register. I previously sent comments about necessary changes to Turnbull as part of the last review in 2005.

The Code and associated guidelines (particularly the Smith Guidelines) need recognise that internal controls are one means of managing risks (Turnbull paragraphs 15 and 16), (So the Smith Guidance (paragraph 4.6) should at least read, *the internal control and* **other** *risk management systems.*)

4. The role of external auditors

In order to prevent the board accepting risks which are likely to threaten the continued existence of the company, the external auditors should be required to confirm that the management of risks is such that it is sufficient to ensure the company is a ‘going concern’.

Biography

I am a qualified Chartered Accountant who was employed by the Boots Group for 27 years. For much of this time I was a manager in the internal audit department and was Group Internal Audit Manager for 6 years, attending the Audit Committee as part of this role. (The Combined Code had not been published in this period, and my comments do not therefore reflect my experience in Boots.) I retired in September 2003. I have been a member of The Institute of Internal Auditors (UK and Ireland) Technical Development Group and a trustee responsible for risk and internal control with an almshouse charity. I have also published a website on risk-based internal auditing (www.internalaudit.biz). I have previously sent comments on the reviews of the Smith and Turnbull Guidelines.

Supporting publications

Implementing Turnbull – a Boardroom Briefing, *ICAEW*

Risk Based Internal Auditing, *Institute of Internal Auditors (UK and Ireland).*

The Role of Internal Audit in Enterprise-wide Risk Management, *Institute of Internal Auditors (UK and Ireland).*

An Approach to implementing Risk Based Internal Auditing, *Institute of Internal Auditors (UK and Ireland).*

Orange Book – The management of risk – principles and concept, *HM Treasury*.

Thinking about risk (3 publications). HM Treasury.