Institute of Internal Auditors
UK AND IRELAND

Mr Chris Hodge
Corporate Governance Unit
Financial Reporting Council
5th Floor Aldwych House
71-91 Aldwych
London, WC2B 4HN

Sent by email to: codereview@frc.org.uk

9 October 2009

Dear Mr Hodge

Review of the effectiveness of the Combined Code – second consultation July 2009

The Institute of Internal Auditors is delighted to have this opportunity to provide our views on the future of the Combined Code.

The role of internal audit includes evaluating and championing improvement in governance processes, including how organisations manage risks. As you know, the Institute of Internal Auditors has made ongoing contributions to the development of the UK's "soft law" approach to improving governance standards. In May this year, we provided detailed input to your review. We are writing now to provide brief additional comments in response to your July paper. These fall into three areas:

- Encouraging responsible risk taking
- Reinforcing good behaviours in non-executive directors
- Restating the core principles of governance

We hope you will find our comments constructive and we would be happy to discuss any of them in more detail. We are content for our comments to be considered as part of the public record.

Yours Sincerely

Dr Ian Peters
Chief Executive

The Institute of Internal Auditors – UK and Ireland Ltd
13 Abbeville Mews, 88 Clapham Park Road, London SW4 7BX
tel 020 7498 0101 fax 020 7978 2492 email info@iia.org.uk
www.iia.org.uk Registered in England and Wales No.1474735

Encouraging responsible risk taking

Managing risk is a core part of management in general. One weakness of the current Combined Code is that the management of risk is subordinated to the issue of control and buried within the Accountability and Audit section. We believe that the Code should recognise the responsibility of the whole board for managing risks by including a new principle and putting it in a separate section from Accountability and Audit.

The Walker Review emphasises the importance of Risk Management by recommending various detailed provisions, such as a separate risk committee and risk reporting to shareholders. The Institute is not convinced that such provisions are valid for all companies and believes that, even for the largest organisations, including Banks and Other Financial Institutions (BOFIs), they carry a grave danger of unintended consequences: having the management of risk disappear into a silo, being seen as the responsibility of the Chief Risk Officer (CRO).

The Institute agrees with the widely held view that "the quality of corporate governance … depends on behaviour not process". Therefore, we do not support provisions that seek to add more process and structures, while threatening to encourage the exact behaviours that we wish to discourage.

What we should be seeking to do is not to separate the management of risk from other activity but rather to link these activities together. The "3 lines of defence" model is clear that the people who are responsible for managing risks are those that are responsible for taking risk – the general management. This is the case in large and small organisations. It is the overriding principle, which is why we recommend that it be reflected in the Combined Code.

We recommend that the highest principle should be that the board is responsible for managing risk. It is the responsibility of the board to agree how best to embed risk into the strategy-setting and decision-making processes of the company. If the board chooses to delegate most of the work to a risk committee, however that is constituted, all directors must understand that, with this as with every responsibility, they cannot delegate their accountability.

Returning to the 3-lines model, the Institute recognises the value of risk management functions. The purpose of these functions is, perversely, not to manage all the risks but to support the business managers – at all levels – in managing risks. The Institute agrees that the services of a professional head of risk management, a CRO, will be valuable to boards. The CRO creates an effective infrastructure and ensures that information flows properly so that managers can take good decisions and so the board can oversee the level of risk being taken. The Institute supports the proposed measures to enhance the independence of the CRO where one exists. However, it may be impractical for smaller companies to support such services, even if they would be useful. Therefore, the Institute recommends that the Code, rather than having a simple provision calling for a risk management function, should establish three principles: firstly, that risk management expertise is valuable; secondly, that larger companies will have a professional CRO; and, thirdly, that the board must take action to support the independence and competence of the CRO if there is one.

The Institute recognises that both Walker and the FRC have concentrated their comments on where they are proposing changes. Therefore, the FRC has have not sought feedback on existing provisions. However, to complete the 3-lines model, the board needs to have

available to it independent and objective assurance from a professional, appropriately resourced, internal audit function. Similar safeguards to those proposed for the CRO are currently granted to the Head of Internal Audit in the FRC's guidance for audit committees. The Institute believes that any principles and provisions that are adopted related to risk management and the CRO should be mirrored with regard to internal audit. So, at a minimum, the Code should establish the principles of the value of internal audit, the expectation that larger companies will have a professional internal audit function and the need for the board to take action to support the independence and competence of the head of internal audit.

In your discussion of the proposals related to risk management, you ask for feedback on the Turnbull guidance. The Institute believes that the Turnbull guidance has been useful. It served to define internal control, not in terms of the objectives it was fulfilling, but in terms of its effectiveness in managing risks. This has promoted a better understanding of internal control. It also provides some guidance on managing risks.

However, the Institute also recognises some concerns with the Turnbull guidance. Firstly, it does not provide a complete approach to managing risk. Secondly, it is linked to the Audit and Accountability section of the Combined Code. Thirdly, and perhaps connected to the last point, matters relating to Turnbull are often seen as the responsibility of the financial control department and relating only to the financial reporting cycle.

The Institute believes that companies will need guidance on how to implement the risk management principles proposed above. It will be much more effective if the guidance on risk management is integrated with the guidance on evaluating the system of internal control, ie the Turnbull guidance, rather than having two documents. Therefore, we recommend that new guidance be developed to support the new and the existing principles.

In summary, the Institute recommends the following:

- The Combined Code should include a principle that the board is responsible for risks being taken by the organisation and for managing them. This principle should not be part of Accountability and Audit.

- The Combined Code should include principles that risk management expertise is valuable; that larger companies will have a professional CRO and risk management function; and that the board must take action to support the independence and competence of the CRO if there is one.

- The Combined Code should have updated principles relating to internal audit: establishing that the availability of independent and objective assurance from internal audit is valuable; that larger companies will have a professional internal audit function; and that the board must take action to support the independence and competence of the head of internal audit if there is one.

- The FRC should ensure that boards have guidance on how to fulfil their responsibilities related to the management of risk as well as to the assessment of the system of internal control. This should be in a single document, replacing the Turnbull guidance.

The aim of all of these principles should be not to stifle risk but to encourage responsible risk taking.

Reinforcing good behaviours in non-executive directors

You ask specifically about how helpful it would be to have guidance on the role, responsibilities and behaviours and on the time commitment of various non-executive directors.

Many of the Walker Reviews recommendations in this area are sensible and supportable in theory. However, it is not always clear how easy they will be to implement or to enforce. At the same time, the Combined Code already covers much of the proposed subject matter.

For example, Recommendation 8 of the Walker Review deals with the competencies of the chairman of a BOFI. It says that, while relevant experience in the industry is valuable, a track record of successful leadership capability is even more important. In our earlier letter, we commented at length on the topic of experience of non-executive directors. We do not wish to repeat those comments. However, we do wish to support this idea that, although experience and knowledge are important, the behavioural competencies can indeed be more important. For the chairman, it is the leadership capabilities that are important. For non-executive directors in general, there are three important attributes: courage, the ability to challenge – to ask what may appear to be the stupid question – and the tenacity to insist on a satisfactory answer.

The Combined Code in Principle A1 states that the role of non-executive directors includes challenging and scrutinising. Later principles and provisions talk about evaluating their strengths and weaknesses; and about the leadership role of the chairman. We recommend that you recognise the qualities above: courage, ability to challenge and tenacity, in one of the supporting principles of section A, perhaps in A6 Performance Evaluation.

The Institute does not support any attempt to specify time commitments for all kinds of company. There are too many variables to take into account and any guidelines are likely to be restrictive without leading to improvements in the performance of the individual directors.

Restating the core principles of governance

The Institute is concerned about the direction that the UK governance regime may take.

On the one hand, the recent crises in governance in the banking sector have created a pressure to do "something". Following that, exercises such as the Walker Review have brought out a number of interesting ideas. It is difficult to argue against the good sense of many of the principles involved, even while it is also difficult to see how they can be implemented and, in particular, enforced.

These bring with them two dangers: firstly, that we are tempted to add extra requirements to reflect all these new ideas; and, secondly, that the requirements will be bolted on to the existing Combined Code and related guidance. Such ad hoc additions will leave the Code disjointed and hard to use.

On the other hand, the Combined Code is not the only statement of the principles of governance in the world today. The "King III" *Code of Governance Principles* from South Africa, the Australian Stock Exchange's *Corporate Governance Principles and Recommendations* and *The Good Governance Standard for Public Services* from The Independent Commission for Good Governance in Public Services in the UK are all high quality documents, which seek to set out a comprehensive list of principles for their

constituencies. They are arguably more complete, coherent and easy to follow than the Combined Code now is.

At the same time, these documents point up some of the weaknesses of the Combined Code. The Code does not identify the organisations to which it is addressed – is it all companies or listed companies only, for example? The Code recognises only one group of stakeholders – the shareholders – despite the broader requirements of the Companies Act 2006. The Code does not give equal weight to all aspects of governance – there is little on how directors direct strategy or manage risks but a great deal on board composition and committee structures and on external auditors.

The Institute does not wish to see the current pressures lead to precipitous action, which will increase the requirements placed on all companies. However, the Institute recognises the need to take action with regard to BOFIs. At the same time, the Institute believes that there would be value in a comprehensive review of the Combined Code in the light of advances in other codes. Such a review should include an aim to simplify and rationalise the requirements – where possible.

Therefore, the Institute recommends the following:

- The FRC should take action to implement relevant recommendations of the Walker Review for BOFIs only. We support the FRC's proposed three guiding principles for this work.

- At the same time, the FRC should plan and implement a more fundamental review of the Combined Code, aiming to simplify and rationalise its requirements and to build a new consensus behind a set of core principles.

Appendix

About the Internal Audit Profession and the Institute

All organisations face risks in everything they do. It is the role of senior management and the board to put in place frameworks and processes to manage risks and to monitor how successful they are at managing them. The profession of internal auditing is fundamentally concerned with providing assurance on the effectiveness of these frameworks, processes and reports.

The internal auditor reports directly and independently to senior managers and to board directors, providing clear evaluations. At the same time, the internal auditor champions effective risk management, challenges those responsible for it on its success and uses knowledge of the business and of the management of risk to catalyse improvements in an organisation's practices.

We therefore define internal auditing as "an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes." [1]

Whilst our members enter the profession from many directions, internal auditing is a distinct, specialist profession with its own unique skill set and a professional qualification structure.

The Institute of Internal Auditors is the only awarding body in the UK and Ireland focused exclusively on internal auditing. The Institute educates internal auditors through its Diploma and Advanced Diploma qualifications. All members are required to follow a Continuing Professional Development (CPD) programme. In addition, the Institute runs a certificated training programme and a range of specialist sort courses.

Established in the UK over 60 years ago, the Institute is part of a global network of 165,000 internal auditors in 165 countries. All members of the network conform to the *International Standards for the Professional Practice of Internal Auditing* and a *Code of Ethics*.

- ENDS -

[1] 1 The Definition of Internal Auditing © 1999 Copyright by The Institute of Internal Auditors, Inc., 247 Maitland Avenue, Altamonte Springs, Florida, 32710-4201 U.S.A.