



Institute of Internal Auditors  
UK AND IRELAND

Sir David Walker  
Financial Services Authority  
25 The North Colonnade  
Canary Wharf  
London E14 5HS

Sent by email to: [feedback@walkerreview.org](mailto:feedback@walkerreview.org)

31 May 2009

Dear Sir David

**Review of Corporate Governance of UK Banking Industry and financial services – initial call for evidence**

The Institute of Internal Auditors plays an active role in the public arena, challenging organisations to reach the highest standards of corporate governance and risk management. We are therefore delighted to have this opportunity to express our views about the future of corporate governance in the UK financial services sector.

The views of the Institute of Internal Auditors – UK and Ireland (IIA) have been developed in consultation with our members. We organise them below in two parts: 1) general views and 2) comments on your terms of reference. In particular, we draw your attention to the following points:

- The credit crunch and the crisis in the financial sector that followed it produced many comments on the importance of risk management to the health of financial institutions. The Institute agrees that risk management is a fundamental requirement – not just of governance but also of management itself. Therefore, the Institute recommends that your review should recognise that the management of risk is a core responsibility of those responsible for governance in financial institutions.
- In addition, we believe that it is necessary to clarify the difference between roles of risk management and assurance functions within financial institutions and, in particular, that risk management functions do not provide assurance. Access to independent and objective assurance is of great value to those responsible for governance. The regulation of some financial institutions does lay down the need for a professional internal audit activity to provide such assurance. The Institute recommends that your review recognises that all financial institutions should have a professional internal audit activity, distinct from risk management, as a fundamental element of good 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

Philip Ratcliffe  
President

## Response from the Institute of Internal Auditors – UK and Ireland

### Review of Corporate Governance of UK Banking Industry and financial services – initial call for evidence

---

#### 1. Introduction

The Institute of Internal Auditors (IIA) is the only body focused exclusively on internal auditing and we are passionate about supporting, promoting and training the professionals who work in it.

We have been leading the profession of internal auditing for over 60 years. Our *International Standards* and *Code of Ethics* unite a global community of 165,000 internal auditors in 165 countries.

The IIA plays an active role in the public arena, building awareness of internal auditing, promoting members' interests and challenging organisations to reach the highest standards of corporate governance.

We are committed to enhancing the recognition and professionalism of internal audit in the UK and in Ireland. To that end, we are consulting with our members and other stakeholders about the award of Chartered status, which will acknowledge qualified internal auditing professionals as experts in their field, offering a clear differentiator between internal audit professionals and others.

## **2. General comments**

### **The need and scope of a review of governance**

The Institute welcomes your review of governance of financial institutions, following both the recent failures in banks and also international advances in thinking on governance. The Institute believes that this is necessary to rebuild the confidence of the international community in the UK's framework.

Given the complexity and fragmentation of the governance framework in the UK, we believe your review has the breadth of scope to improve governance as a whole. Although you are looking at the governance of financial institutions in particular, we think it likely – and beneficial – that your recommendations will resonate for other sectors as well. In addition, our members are strongly of the view that the same principles of governance should apply to all organisations. Our comments are, therefore, somewhat generic in nature. We have made similar comments to the Financial Reporting Council in response to their call for evidence on the review of the effectiveness of the Combined Code.

The profession of internal auditing recognises that governance is fundamental to the chances of organisations meeting their objectives, which is our ultimate aim. This is because governance sets the scene for and embraces effective risk management, including control. Our comments are particularly focused on those areas of governance that directly affect the effectiveness of risk management.

### **Fragmentation of governance framework in the UK**

The governance framework in terms both of the content of governance and of the enforcement of best practice is fragmented in the UK. Many people believe that governance is only about the matters that are discussed in the Combined Code. However, from international sources it is clear that governance includes other subjects. In our framework these are dealt with in legislation or regulation and include topics such as shareholders' rights and the enforcement of accountability through disclosures of directors' remuneration and governance and risk management practices.

This fragmentation is even more obvious for financial institutions. They are constituted under different Acts of Parliament and are subject also to the regulations of the Financial Services Authority. Listed institutions have the Listing Rules, including disclosure requirements related to the Combined Code. Those responsible for governance of the institutions may have different titles and their duties and responsibilities and qualifications are to be found across statute, regulation and code.

We have no evidence to suggest that this fragmentation has caused poorer standards of governance than necessary. However, it seems logical that a more streamlined and coherent approach would help both those responsible for governance and also their stakeholders and will, all other things being equal, improve the effectiveness of governance.

## **Response from the Institute of Internal Auditors – UK and Ireland**

### **Review of Corporate Governance of UK Banking Industry and financial services – initial call for evidence**

---

#### **The importance and limitations of governance**

The Institute believes that organisations that apply the principles of good governance are more likely to achieve the objectives of their owners and other stakeholders over time than those that do not. Therefore, in general, we support the efforts to improve governance in any sector.

However, the Institute also recognises the limitations of governance. Well governed organisations can make mistakes. More importantly, risks can crystallise and threaten the survival of the organisation even if it is well governed.

The existence of systemic risks may make this more likely. Those responsible for governance of individual institutions will struggle to manage systemic risks. We recognise that the Turner Review has dealt with this in detail and we will be providing comments to the Financial Services Authority in due course.

The Institute believes that it is important that we do not burden the governance framework with unrealistic expectations. To that end, we set out in the next section a high level summary of the overriding principles and elements of governance.

#### **The overriding principles and elements of governance**

Governance is about the control and direction of organisations.

The first question that needs to be clarified is: control and direction for whose good? The Combined Code on Corporate Governance, in its preamble, focuses on shareholders. The Companies Act 2006 implies that there is a role for a wider group of stakeholders given contents of the Section 172 duty to promote the success of the company for the benefit of its members as a whole. Further afield, the draft Code of Governance Principles for South Africa – 2009 from the King committee on governance (King III) is explicit in the importance of other stakeholders.

The Institute recommends that your review considers this question. The answer to the question will affect the type of regulation and enforcement that is needed for the governance framework.

The overriding principles of good governance are accountability, transparency, probity and equity. These can sometimes be obscured by the detail of legislation, regulations and codes. The Institute believes that this is a good opportunity to reassert the fundamentals and to establish their pre-eminence to guide the behaviour of managers and those responsible for governance in financial institutions.

The core activities related to governance include setting direction and establishing the foundation for control in its widest sense; accepting accountability; taking decisions and making judgments with probity; making reports to stakeholders communicating the strategy and reporting on progress and performance as part of transparency; and treating stakeholders fairly or equitably. They also include providing mechanisms for appointing and holding to account key individuals such as directors, external auditors and internal auditors. The diversity of these activities bring home again the idea that our current governance framework is fragmented.

A comprehensive review should survey all of the aspects of governance even if some of these aspects do not need to be improved. Otherwise, action and energy will be spent on current issues, and problems could develop in other areas in the future.

## **Response from the Institute of Internal Auditors – UK and Ireland**

### **Review of Corporate Governance of UK Banking Industry and financial services – initial call for evidence**

---

#### **Control**

Control must not be interpreted too narrowly. It is often understood in the context of financial reporting controls and other detailed checks that are the province of accountants. However, if strategy and society's expectations provide the organisation's objectives, then achieving those is the aim of "control". To achieve control, the organisation needs to identify and manage the risks to all those objectives. There needs to be clear accountability for these objectives and for all the related control activities.

The Institute would also draw your attention to the importance of behavioural aspects of objectives, risks and control. These aspects may be harder to quantify and assess but they are vital to good governance.

Many of the aspects of transparency have been focused up to now on financial reporting. It is time to ensure that information on strategy, performance and risks also has a place. This is the responsibility of all of those responsible for governance, not just the audit committee. The audit committee may undertake some of the work but the governors cannot delegate responsibility.

When it comes to assurance as well, the external auditor provides assurance to the shareholders so that they have more confidence in the reporting by the governors. However, this does not wipe out the shareholders' responsibility to take care; nor the governors' responsibility to report accurately.

Similarly, an effective governance system will have checks and balances. It will include information flows up to the governors, including the provision of objective assurance, provided independently of those responsible for executing and operating the organisation. Professional internal audit can provide such assurance. However, the existence of such assurance does not remove the responsibility of all the governors for the effective performance of the financial institution – and for the management of its risks.

#### **Public interest role of those responsible for governance**

Within statute, regulation and code there are varying duties laid upon directors and others responsible for governance. For example, the Combined Code focuses on the role of directors in directing and controlling companies for the benefit of shareholders, including setting directors' remuneration in order to align their objectives with those of the company. However, the Companies Act 2006 gives directors a wider duty to consider the success of the company and to consider the requirements of other stakeholders too.

In your wider view, it would be good to consider the question whether those responsible for the governance of financial institutions should limit themselves to looking after their shareholders or members, or whether they should also have a public interest role.

It may be considered too onerous to require all those responsible for governance to play this role. Perhaps there would need to be a spectrum based on the nature of the organisations they run and their impact on society as a whole. So, at the extreme, institutions that are "too big to fail" would have to have to appoint some governors present people who have an eye for the public interest. These governors would need to understand how the risks to the wider stakeholders, including society as a whole, are being managed and would wish to receive assurance on the effectiveness of this management.

## **Response from the Institute of Internal Auditors – UK and Ireland**

### **Review of Corporate Governance of UK Banking Industry and financial services – initial call for evidence**

---

#### **‘Comply-or-explain’ – enforcement**

Whatever the requirements of governance are, there will still be a need to enforce them in some way.

‘Comply-or-explain’ has come to represent the governance framework used in the UK and is used by many commentators to represent a principles-based approach in contrast to a rules-based one.

However, international developments have moved away from this phrase, partly because many organisations feel that the word “comply” implies that there is little flexibility – the very opposite of the intention here. A variety of phrases are now in use: “comply or explain”; “adopt or explain” and “apply or explain”. A fuller explanation of the arguments is provided in the introduction to the draft Code of Governance Principles for South Africa – 2009 from the King committee on governance (King III).

Furthermore, although the phrase has served as a useful sound bite, it does not actually explain the situation in the UK. There is no all-encompassing requirement to comply with the Combined Code or explain the non-compliance. Companies listed on the London Stock Exchange are required by the listing rules, not to comply, but to make disclosures about their compliance. In fact, listed companies are required to explain how they apply the principles, which might be thought to be the most important part of the Code. In addition, they must disclose whether or not they comply with the provisions. Therefore, companies face penalties from their market regulator only if they fail to disclose.

Clearly, this reinforces the idea that the main mechanism for enforcing good standards of governance is via the market and the main players are the investors and members. However, as we note below, this may not be enough if we accept that companies have other stakeholders whose interests need protecting.

To add to the complications here, financial institutions, because of the fragmented framework discussed above, do not all face the same enforcement mechanisms. Those that are listed companies are subject to the regime above; others are regulated more directly by the Financial Services Authority. The Institute believes it would be useful to have a full survey of the enforcement mechanisms.

#### **Fundamental responsibility for risk management**

The Institute supports the view that risk management is a fundamental requirement for the successful management and governance of organisations. Those responsible for governance should have a clear accountability for risk management.

The Institute would like to emphasise that there are three distinct aspects to the management of risk.

Firstly, we believe that risk management is an essential part of management. Everyone in an organisation has a role to play in identifying and responding to risks; and for managers, part of their responsibilities as managers is managing risks, including monitoring how well risk responses are working and reporting on that up the line in some way that enforces their accountability. This is the heart of risk management.

## **Response from the Institute of Internal Auditors – UK and Ireland**

### **Review of Corporate Governance of UK Banking Industry and financial services – initial call for evidence**

---

Secondly, there are specialist “risk management functions” who support the line managers with this work. They facilitate risk management activities in general by measuring, monitoring and reporting on the extent to which risk appetite and risk tolerances are met or exceeded and providing a challenge that is independent of those incurring the risk. They assist organisations to be consistent in their risk management activities. However, the activities all form part of the ongoing risk management process and should they cease to function, the organisation would not be able to manage its risks effectively day to day.

Thirdly, internal audit provides assurance activities that are part of the governance process but sit outside of the risk management process. These activities regularly conclude on the effectiveness of each element of the process and of the process overall. Internal audit may (and indeed should) use the outputs of risk management activity in forming its conclusions. Assurance activity is effective only where it is independent of all elements of the risk management process. Should assurance activity cease, the organisation would be able to continue to manage its risks effectively day to day, but we would question the effectiveness of the organisation’s governance.

Therefore, the Institute believes that those responsible for the governance of financial institutions are responsible for risk management and also, as the next heading demonstrates, require access to independent and objective assurance from a professional internal audit activity. We believe that it is important to clarify that these are separate and distinct activities.

#### **Importance of independent and objective assurance – internal audit**

In undertaking all of their responsibilities, those responsible for governance are dependent upon receiving information. It is not just the information itself that is necessary but a way of understanding the relevance and reliability of that information. The availability of independent and objective assurance from professional internal auditors can assist the governors in understanding these aspects and can help them in formulating their overall views on the effectiveness of the system of internal control.

Much of the regulatory framework for financial institutions provides some recognition of the value of internal audit. It is also a specific section of the draft King III. The Institute recommends that a professional internal audit activity be recognised as an essential part of the governance framework for all financial institutions.

### 3. Detailed comments related to your terms of reference

#### **The effectiveness of risk management at board level, including the incentives in remuneration policy to manage risk effectively**

The Institute believes that there is a varied standard of understanding amongst boards of their responsibilities related to risk management and that, frequently, only lip service is paid to this requirement.

The board is responsible for setting the tone for risk management. Part of setting the direction of the company is about deciding how much risk to accept – the risk appetite. Part of controlling the company is establishing an open culture with the right incentives and providing adequate resources so that managers can identify, respond to, monitor and report on risk. The board is responsible for forming a view of the company's management of risk. The board can do this in a complex organisation only by receiving and reviewing reports from the organisation. To assess these, it needs to understand the business.

This is where risk management becomes particularly difficult for those responsible for governance in financial institutions. The nature of risk and the way it is modelled and managed are complex. The operations are abstract and have limited transparency for many people. At the same time, new financial products are easy to create and launch and can result in the accumulation of positions which are both obscure and highly risky in their net impact.

This is the right time to open a dialogue about the complexity of risk management and about the importance of behavioural aspects, not just processes. However, our members advise caution in any recommendations related to incentivising effective management of risk. Because effective management of risk depends on human behaviour and can be difficult to measure, any link between the effective management of risk and remuneration may be extremely difficult to implement and there is a huge risk that unintended consequences may follow a too simplistic scheme.

For example, it might motivate individuals to ignore risks that are difficult to measure or to manage because these would reduce remuneration.

#### **The balance of skills, experience and independence required on the boards of UK banking institutions**

The Institute believes that directors of companies and others responsible for governance of other institutions need to understand the business, to have an independence of mind – or objectivity – and to have courage and tenacity to ask questions and to insist on answers.

There is some concern that the implementation of the Combined Code has led to a reduction in the number of executive directors on boards and to a proliferation of independent non-executive directors who have little knowledge or experience of the financial services sector.

The Institute believes that independence as defined by the Code does not guarantee objectivity although we accept that objectivity may be impaired by a loss of independence. We believe that your review should focus on the outcome that is desired: the mix of skills and characteristics that those responsible for governance need, rather than on the processes to appoint them.

## **Response from the Institute of Internal Auditors – UK and Ireland**

### **Review of Corporate Governance of UK Banking Industry and financial services – initial call for evidence**

---

#### **The effectiveness of board practices and the performance of audit, risk, remuneration and nomination committees**

This is a broad question. The Institute's main concern is that it is the board of directors – or its equivalent in other financial institutions – that is accountable for the activities that are undertaken by the committees. The committees provide more time to devote to the activities and leave the board free to consider other matters. However, all directors should be conscious of their accountability for the issues.

#### **The role of institutional shareholders in engaging effectively with companies and monitoring of boards**

Institutional shareholders have a role in promoting standards of good governance only in financial institutions with institutional shareholders.

Even there, the Institute believes that it is not appropriate to rely on this group to enforce such standards, since this creates a conflict of interest for those investors.

Institutional investors may or may not wish to hold investments over the long term. If they do, then this provides a motivation to engage with companies where standards of governance do not meet the investors' requirements.

However, it is also entirely reasonable for investors to react to companies' actions by selling the shares of companies with whose actions they do not agree, not by engaging with them. This may serve to signal to the directors that their governance standards are not adequate. However, this message may be lost in others, not least because investors have many other reasons for buying and selling shares.

#### **Whether the UK approach is consistent with international practice and how national and international best practice can be promulgated**

It is difficult to compare international practice in all aspects because of the fragmentation of our governance framework.

- ENDS -