Effective Internal Audit in the Financial Services Sector

Draft recommendations to the Chartered Institute of Internal Auditors

11 February 2013
## Contents

1. Covering Letter ...................................................................................................................................... 1
2. Introduction and Background ............................................................................................................... 2
3. Committee Membership ....................................................................................................................... 3
4. Proposed Recommendations of the Committee................................................................................... 4
1. Covering Letter

Following the crisis in the financial system over the past few years a wide spread review of governance in financial institutions has been taking place. It was inevitable that the role of Internal Audit would be brought into that process. Whilst there has not been extensive criticism of Internal Audit’s part in the financial crisis, some would say that this reflects too low an expectation of what Internal Audit could, and should have, delivered.

Given this, and a number of individual failings detected during the regulatory process, the Financial Services Authority requested that the Chartered Institute of Internal Auditors develop a code to set out the expectations of internal audit functions in the financial sector.

I was therefore pleased to have been invited by the Institute to chair a Committee aimed at identifying reasonable expectations of internal audit in UK financial institutions. I was also very pleased that we were able to attract a range of highly qualified people on to the Committee. The Committee includes not only internal audit directors but also non-executive directors and people with skills in executive and risk management, regulation and governance.

Of course internal auditors already work in compliance with standards promulgated by the Institute. However these standards are not industry specific and in particular do not meet all the current expectations of internal audit in significant UK financial institutions.

In this document, we set out recommendations to the Chartered Institute which, we believe, address these expectations. These recommendations for the most part supplement, rather than replace, the existing standards. They are informed not only by the work of the Committee but also by the significant and thoughtful responses to our call for evidence.

These responses, and a number of meetings with internal audit directors of large banks and insurance companies, have impressed me with the quality of work performed by internal audit. Whilst there were doubtless examples of poor internal audit work, and ineffective internal audit functions, leading up to the financial crisis I do not subscribe to the view that all internal audit functions are in drastic need of improvement. However these draft recommendations, if implemented, are likely to lead to significant change for some organisations and are likely to affect all internal audit functions of UK financial institutions to some extent.

Emphasising the need for proportionality we have kept the draft recommendations at a fairly high level. Whilst we believe that the recommendations are relevant to internal audit functions in all UK financial institutions, and the UK operations of overseas institutions, the detailed recommendations may not all be applicable in smaller institutions. We also stress that implementation of some of these recommendations is a matter for the Board; Internal Audit cannot deliver them by themselves.

We now welcome comments on this draft Guidance, at the latest by 12 April 2013, which will be made publicly available via the IIA website after the consultation period. All responses to this document should be sent to Chris Spedding, Secretary to the Committee, via chris.spedding@iia.org.uk. We will be holding a number of open meetings in March to receive oral feedback and are very open to individual meetings.

Roger Marshall

Chairman of the Committee
2. Introduction and Background

The recommendations included in the following Guidance are made by the Committee to the Chartered Institute of Internal Auditors in the UK and are designed to provide a benchmark for effective Internal Audit in Financial Services in the UK. The intended audience for this Guidance includes Chief Internal Auditors, Executive and Non-Executive Directors and the Regulatory bodies.

The Guidance should be applied in conjunction with the existing Institute of Internal Audit International Professional Practices Framework (IPPF), which includes the International Standards for the Professional Practice of Internal Auditing (the IIA Standards). It includes some elements covered by the Basel Committee on Banking Supervision’s paper on the Internal Audit functions in banks.

The recommendations are designed to provide incremental Guidance to existing standards, such as the IIA Standards and Basel paper. In the course of the Committee consultation, and through discussion with the regulator’s supervisory teams, examples of non-conformance to these existing standards were identified. These include key risk areas that were not included in the scope, risk assessment and audit plan of Internal Audit; audit opinions (particularly “satisfactory” audit opinions) with insufficient work and/or evidence of work to fully support and justify the opinion; and audits in which the audit work programme included the operating effectiveness, but not the design adequacy, of processes and controls. The Committee views these instances as examples of Internal Audit practice that does not meet the existing IIA Standards and expectations of the profession, as opposed to areas requiring incremental Guidance. The Committee emphasises the importance of full conformance to the attribute and performance principles, as defined in the IIA Standards, as the basis for robust Internal Audit.

The consultation process through which this Guidance was created sought input from a range of stakeholders with interest in the risk management, governance and control of financial institutions. This included the Chartered Institute of Internal Auditors; the Bank of England; the Financial Services Authority (representatives from both the future Prudential Regulation Authority and the Financial Conduct Authority); audit practitioners from across the sector, including banking, insurance, asset management and building societies; Executive and Non-Executive Directors of financial organisations; government representatives; rating agencies; professional services firms; and consumer groups.

In the course of our consultation, the Committee asked a range of questions around the role, scope and position of internal audit in the organisation's governance and risk management frameworks. The responses received highlight the range of practice across the industry, with a varying degree of uniformity of practice and aspiration between organisations.

There was a general consensus around the importance of the independence of Internal Audit; both independence from Executive Management authority, from the Risk Management and Compliance functions, and from executive decision making responsibilities. There was also strong support for an unrestricted scope of Internal Audit, and for greater clarity and consistency of Internal Audit’s role in auditing areas such as strategy, culture, risk appetite and key corporate events.

Areas in which there was a greater divergence of response include the role and extent of Internal Audit involvement in challenging strategic decision making; whether there are circumstances in which it would be appropriate for Internal Audit to report to a Board Risk Committee rather than to the Audit Committee, the nature of Internal Audit’s Executive reporting line and who this line should report into (e.g. CEO / CFO); and the appropriateness of the Chief Internal Auditor having the right to attend Executive Committee meetings. In these areas, the Committee has formed a view based on both the responses received and Committee discussion.
### Committee Membership

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roger Marshall (Chair)</td>
<td>Audit Committee Chair, Old Mutual, Director, Financial Reporting Council (FRC)</td>
</tr>
<tr>
<td>Brendan Nelson</td>
<td>Audit Committee Chair, BP, Audit Committee chair, RBS</td>
</tr>
<tr>
<td>Paul Boyle</td>
<td>Chief Audit Officer, Aviva (formerly chief executive Financial Reporting Council)</td>
</tr>
<tr>
<td>Paul Lawrence</td>
<td>Group General Manager, Internal Audit, HSBC</td>
</tr>
<tr>
<td>Martyn Scrivens</td>
<td>Group Chief Auditor, Credit Suisse</td>
</tr>
<tr>
<td>Carol Sergeant</td>
<td>Former Chief Risk Officer, Lloyds Banking Group (formerly, Managing Director of the Regulatory Process and Risks Directorate at the Financial Services Authority)</td>
</tr>
<tr>
<td>Prof. Andrew Chambers</td>
<td>London South Bank and Birmingham University, expert on corporate governance and internal audit, adviser to 2010-11 House of Lords inquiry into audit market concentration</td>
</tr>
</tbody>
</table>
4. Proposed Recommendations of the Committee

A. Role and mandate of Internal Audit

1. The primary role of Internal Audit should be to help to protect the assets, reputation and sustainability of the organisation. It does this by assessing whether all significant risks are identified and appropriately reported to the Board and Executive Management; assessing whether they are properly controlled; and by challenging Executive Management to improve the effectiveness of governance, risk management and internal controls. The role of Internal Audit should be articulated in an Internal Audit Charter, which should be publicly available.

B. Scope and priorities of Internal Audit

2. Internal Audit’s scope should be unrestricted. In setting its scope, Internal Audit should independently determine the key risks that face the organisation, including emerging and systemic risks, and how effectively these risks are being managed. There should be no impediment to Internal Audit’s ability to challenge the executive and to report its concerns.

3. For the avoidance of doubt, Internal Audit should include within its scope:

   a. The design and operating effectiveness of governance structures and processes of the organisation.

   b. The strategic and management information presented to the Board

      Internal Audit should include within its scope the processes and controls supporting strategic decision making, and based on this work, whether the information presented to the Board and Executive Management is complete, accurate and fairly represents the benefits, risks and assumptions associated with the strategy and associated business model.

   c. The setting of, and adherence to, risk appetite

      Internal Audit should assess whether the risk appetite has been established and reviewed through the active involvement of the Board and Executive Management, and is accurately embedded within the activities, limits and reporting of the organisation’s businesses.

   d. The risk and control culture of the organisation

      Internal Audit should include within its scope the risk and control culture of the organisation. This should include assessing whether the processes (e.g. appraisal and remuneration) and actions (e.g. decision making) are in line with the values, ethics, risk appetite and policies of the organisation.

      Internal Audit should consider the attitude and assess the approach taken by all levels of management to risk management and internal control. This should include management’s actions in addressing known control deficiencies as well as their regular assessment of controls within their areas.
e. Risks of poor customer outcomes, giving rise to conduct or reputational risk

Internal Audit should evaluate whether products, services and supporting processes are designed in line with conduct regulation, and the organisation’s customer strategy, values and standards. Internal Audit should evaluate whether the organisation is acting with integrity in its dealings with all customers and in its interaction with relevant markets.

f. Capital and liquidity risks

Internal Audit should include within its scope the management of the organisation’s risks relating to capital and liquidity and other regulatory risks.

g. Key corporate events

These events include significant business process changes, introduction of new products and services, outsourcing decisions and acquisitions/divestments. Internal Audit should decide if these events are sufficiently high risk to warrant involvement on a real time basis. In doing so Internal Audit will evaluate whether the key risks are being adequately addressed (including by other forms of assurance, e.g. third party due diligence) and reported. Internal Audit should also assess whether the information being used in the decision making is, to the extent possible, complete, accurate and balanced and whether the related procedures and controls have been followed.

h. Outcomes of processes

Internal Audit should evaluate the adequacy and effectiveness of the design, as well as the implementation, of the organisation's policies and processes. As part of this evaluation, Internal Audit should consider whether the outcomes achieved by the implementation of these policies and processes are in line with the objectives, risk appetite and values of the organisation.

4. Prioritisation of Internal Audit work

Internal Audit should make a risk-based decision as to which areas within its scope should be included in the audit plan – it does not have to cover all of the potential scope areas every year.

In setting its priorities and deciding where to carry out more detailed work, Internal Audit should focus on the areas where it considers risk to be higher, as well as taking into account the wishes of the Board and Board Committees. Both the determination and the assessment should be informed, but not driven, by the views of management or the Risk function.

5. Risk assessment

Internal Audit’s risk assessment should be all-encompassing, taking into account business strategy and objectives and the full range of risks that have an impact on the organisation; combine a bottom up and top down assessment of risk; and take into account potential future or emerging risks on a continuous basis.

6. Internal Audit planning

Internal Audit plans should be approved by the Audit Committee*. They should have the flexibility to deal with unplanned events to allow Internal Audit to prioritise emerging risks. Changes to the audit plan should be considered in light of Internal Audit’s ongoing assessment of risk. Items removed from Internal Audit’s plans should be reported, with appropriate justification, to the Audit Committee*. 
C. Reporting results

7. Internal Audit should be present at, and issue reports to, both the Board Audit Committee and the Board Risk Committee and any other Board Committees as appropriate. The nature of the reports will depend on the remits of the respective Committees.

8. Internal Audit’s reporting to the Audit and Risk Committees should include:
   - a focus on significant control breakdowns together with a robust root-cause analysis;
   - any thematic issues identified across the organisation;
   - an independent view of management’s reporting on the risk management of the organisation, including a view on management’s remediation plans (which might include restricting further business until improvements have been implemented) highlighting areas where there are significant delays; and
   - at least annually an assessment of the overall effectiveness of the governance, and risk and control framework of the organisation, together with an analysis of themes and trends emerging from Internal Audit work and their impact on the organisation’s risk profile.

D. Interaction with Risk Management, Compliance and Finance

9. Internal Audit should not be part of, nor responsible for, the Risk Management, Compliance or Finance function.

10. Internal Audit should include within its scope an assessment of the adequacy and effectiveness of the Risk Management, Compliance and Finance functions. In evaluating the effectiveness of internal controls and risk management processes, in no circumstances should Internal Audit rely exclusively on the work of Risk Management, Compliance or Finance. Internal Audit should always examine for itself, an appropriate sample of the activities under review.

11. Internal Audit should exercise informed judgement as to when to place reliance on the work of Risk Management, Compliance or Finance. To the extent that Internal Audit places reliance on the work of Risk Management, Compliance or Finance function, that should only be after a thorough evaluation of the effectiveness of that function in relation to the area under review.

E. Independence and authority of Internal Audit

12. The Chief Internal Auditor should be at a senior enough level within the organisation (normally expected to be at Executive Committee or equivalent) to give him or her the appropriate standing and authority to challenge the Executive. Subsidiary and divisional Heads of Audit should also be of a seniority comparable to the senior management whose activities they are responsible for auditing.

13. Internal Audit should have the right to attend Executive Committee meetings and any other key management and decision making fora. This right of attendance is for the duration of the meeting, and will enable Internal Audit to gain an understanding of the business and provide perspectives on risk and control.

14. Internal Audit should have sufficient and timely access to key management information and a right of access to all of the organisation’s records, necessary to discharge its responsibilities.

15. The primary reporting line for the Chief Internal Auditor should be to the Chairman of the Board of Directors. The Chairman may wish to delegate responsibility for the reporting line to the Chairman of the Board Audit Committee or, exceptionally, the Chairman of the Board Risk Committee, providing this Committee is constituted exclusively of independent Non-Executive
Directors. The reporting line should take into account the respective mandates of the Board Audit Committee and the Board Risk Committee, and must avoid any impairment to internal audit's objectivity.

16. The Audit Committee* should be responsible for appointing the Chief Internal Auditor and removing him/her from post.

17. The Chairman of the Audit Committee* should participate in setting the objectives of the Chief Internal Auditor and appraising his/her performance although it would be expected that the objectives and appraisal would take into account the views of the Chief Executive.

18. The Chairman of the Audit Committee* should be responsible for recommending the remuneration of the Chief Internal Auditor. The decision should be ratified by the Remuneration Committee. The remuneration of the Chief Internal Auditor and Internal Audit staff should be structured in a manner such that it avoids conflicts of interest, does not impair their independence and objectivity and should not be directly linked to the short term performance of the organisation.

19. Subsidiary and divisional Heads of Audit should report primarily to the Group Chief Internal Auditor, except insofar as prohibited by local legislation or regulation. This includes the responsibility for setting budgets and remuneration, conducting appraisals and reviewing the audit plan.

20. In order to protect the objectivity and independence of Internal Audit, the Audit Committee* should determine an appropriate interval to consider the need to change the Chief Internal Auditor and should have a similar policy for divisional and subsidiary heads.

21. If Internal Audit has a secondary Executive reporting line, this should be to the CEO in order to preserve independence from any particular business area or function.

F. Resources

22. The Chief Internal Auditor should ensure that the audit team has the skills and experience commensurate with the risks of the organisation. This may entail recruitment, secondment from other parts of the organisation or co-sourcing with external third parties.

23. The Chief Internal Auditor should provide the Audit Committee* with a regular assessment of the skills required to conduct the work needed, and whether the Internal Audit budget is sufficient to allow the function to recruit and retain staff with the expertise and experience necessary to provide effective challenge throughout the organisation and to the executive.

24. The Audit Committee* should be responsible for approving the Internal Audit budget.

25. The Board of Directors should confirm in the annual report that it is satisfied that Internal Audit has the appropriate resources.

G. Quality assessment

26. The Board or the Audit Committee* is responsible for evaluating the performance of the Internal Audit function on a regular basis. In doing so it will need to identify appropriate criteria for defining the success of Internal Audit. Delivery of the audit plan should not be the sole criterion in this evaluation.

27. Internal Audit should maintain an up-to-date set of policies and procedures, and performance and effectiveness measures for the Internal Audit function. Internal Audit should continuously improve these in light of industry developments.
28. Internal Audit functions of sufficient size should develop a quality assurance capability, with the work performed by individuals who are independent of the delivery of the audit plan. The function should have the standing and experience to meaningfully challenge Internal Audit performance and to ensure that Internal Audit judgements and opinions are adequately evidenced. The quality assurance review should include Internal Audit's understanding and identification of risk and control issues, in addition to the adherence to audit methodology and procedures. This may require the use of resource from external parties. The quality assurance work should be risk-based to cover the higher risks of the organisation and of the audit process. The results of these assessments should be presented directly to the Audit Committee* at least annually.

29. In addition the Audit Committee* should obtain an independent, external assessment at appropriate intervals. This could take the form of periodic reviews of elements of the function, or a single review of the overall function. The conformance of Internal Audit with the recommendations included in this Guidance should be explicitly included in this evaluation. The Chairman of the Audit Committee* should oversee and approve the appointment process for the independent assessor.

H. Relationships with Regulators

30. Nature and purpose of the relationship

The Chief Internal Auditor, and other senior managers within Internal Audit, should have an open, constructive and co-operative relationship with regulators which supports sharing of information relevant to carrying out their respective responsibilities.

31. Compliance with the Statements of Principle and Code of Practice for Approved Persons, and the UK Corporate Governance Code

As a significant influence function, the Chief Internal Auditor must fully comply with the relevant provisions of the Statements of Principle and Code of Practice for Approved Persons, the UK Corporate Governance Code, and other obligations specific to Internal Audit as set out in the relevant regulator's handbook.

I. Wider considerations

32. The Board Committees and senior management should set the right "tone from the top" to ensure support for, and acceptance of, Internal Audit at all levels of the organisation.

33. The Financial Reporting Council should consider whether additional guidance is needed with regard to the respective role and mandate of the Board Audit and Risk Committees in relation to their interaction with Internal Audit, including what should be expected from a good Internal Audit function with reference to the recommendations included in this Guidance.

* In the interest of simplicity and clarity, this document has assumed that Internal Audit’s primary reporting line is to the Audit Committee. Please refer to recommendation 15 for the Committee recommendation relating to Non-Executive reporting lines.
About the Chartered Institute of Internal Auditors (IIA)

The 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 65 years. Our International Standards and Code of Ethics unite a global community of over 180,000 internal auditors in 190 countries. We are committed to enhancing the recognition and professionalism of internal audit in the UK and Ireland, through:

- Dynamic leadership of the profession which maximises our members’ reputation and influence individually and collectively.
- Technical excellence through our International Standards and Code of Ethics.
- All members across the globe work to the same International Standards and Code of Ethics.
- We have 8,000 members in all sectors in the UK and Ireland.
- High quality support to our members throughout their careers, which enables them to continually develop their professional knowledge, skills and experience and provides other services of value to members in their roles.

These things, enacted through our staff, members and volunteers and with the support of our suppliers and partners, make a significant and unique contribution to the success of all organisations.