WHAT EVERY DIRECTOR SHOULD KNOW

How to get the most from your internal audit
Foreword

This is the second edition of our flagship governance guide – “What every director should know”. Since we published the original in April 2013, the Financial Reporting Council has revised the Corporate Governance Code and published new guidance on risk management and internal control, the UK and Ireland governments have rolled out comprehensive internal audit standards, and the IIA has produced a Code of good practice for internal audit in the UK financial services sector. These are having a significant impact on the governance of internal audit and the expectations boards are placing on it.

This new version of our guide reflects these changes. It has also been expanded to cover new topics of direct relevance to boards, and in particular audit committee chairs, such as the audit of culture, risk-based internal auditing, and evaluating the effectiveness of the function. As before, we are grateful to the IOD for endorsing this publication.

Internal audit is the eyes and ears of the board and its committees, above all its audit committee. Working independently of management, internal audit provides objective assurance to directors that, in the pursuit of the company’s objectives, risks are being managed effectively, financial and other controls are in place, and the organisation is being properly governed. Here are ten essential actions for boards to take to ensure that their organisation maximises internal audit’s value and gains maximum protection and assurance from its activities.

In many organisations, board responsibility for internal audit has been devolved to an audit committee, and we therefore address this guidance to audit committees. However, the information is just as relevant for other board members, especially the chair, and senior members of the executive, notably the Chief Executive Officer. While some of the terminology used in this guidance relates to the private sector, organisations in the public sector and third sector should also find it invaluable.

Dr Ian Peters
Chief Executive
April 2015

Contents

3 Ten ways to get the most from internal audit
4 How internal audit works for you
6 Internal audit and the governance of risk – the three lines of defence
8 Top 10 recommended practices for effective internal audit oversight
18 Annex 1 – Sample internal audit charter
20 Annex 2 – Sample audit committee charter
22 Annex 3 – What makes an effective Head of Internal Audit?
23 Annex 4 – Evaluating the effectiveness of internal audit
25 Annex 5 – What is Risk-Based Internal Audit?
27 Annex 6 – Culture and the role of internal audit
29 Annex 7 – Whistleblowing and corporate governance
## Ten ways to get the most from internal audit

1. Take responsibility for the provision of internal audit, including whether to have it and how it is provided.
2. Assess and approve the internal audit charter (terms of reference) and review regularly.
3. Ensure a close working relationship with the Head of Internal Audit, promoting effective formal and informal communication.
4. Assess the resourcing of the internal audit function.
5. Monitor the quality of internal audit work, both in-house and external.
6. Evaluate, approve and regularly review the risk-based annual internal audit plan.
7. Oversee the relationship between internal audit and centralised risk monitoring.
8. Ensure the collective assurance roles of internal audit, other internal assurance providers and external audit, are coordinated and optimised.
9. Assess internal audit findings and the breadth and depth of internal audit reports.
10. Monitor management implementation of internal audit recommendations.
How internal audit works for you

Internal audit is a key component of corporate governance – the eyes and ears of the board and its committees, above all the audit committee. When properly resourced, positioned and targeted, internal audit gives an unbiased and objective helicopter view of what is happening in the organisation. Working independently of management within the organisation, internal audit provides assurance that, in the pursuit of the company’s objectives, internal controls are operating, risks are being managed effectively within the defined risk appetite, and the organisation is being properly governed.

Effective corporate governance

The IIA International Standards define governance as “the combination of processes and structures implemented by the board in order to inform, direct, manage and monitor the activities of the organisation toward the achievement of its objectives”.

According to the Financial Reporting Council’s (FRC’s) UK Corporate Governance Code, the purpose of corporate governance is to facilitate effective, entrepreneurial and prudent management that can deliver the long-term success of the company. Strong corporate governance relies on robust processes for reporting, risk management and internal control. According to the Code, directors should monitor the company’s risk management and internal control systems and, at least annually, carry out a review of their effectiveness, and report on that review in the annual report.

Culture, values and ethics are increasingly important considerations in the governance of organisations. For the first time the 2014 edition of the Corporate Governance Code highlights a key role for the board in establishing culture, values and ethics, considering among other things the culture it wishes to embed, and whether this has been achieved. It is not sufficient for the board simply to set the desired values. The board also needs to ensure they are communicated by management, incentivising the desired behaviours and sanctioning inappropriate behaviour, and must assess whether the desired values and behaviours have become embedded at all levels.

In many organisations audit committees are charged with overseeing, on behalf of the board, the quality of all the above processes. Indeed the establishment of an audit committee is a requirement of the Corporate Governance Code for publicly listed companies on a comply-or-explain basis. In other organisations the board and its individual directors will retain some or all of the functions of committees of the board, such as the audit or risk committee.

Internal audit – a vital tool of the audit committee

The audit committee’s tasks include reviewing the company’s internal controls and, unless expressly addressed by a separate board risk committee composed of independent directors or by the board itself, reviewing the company’s governance and risk management systems. To do this, it utilises the skills and expertise of the internal audit function, agreeing the scope of its work, its priorities and resources.

It must also monitor and review the effectiveness of the organisation’s internal audit function. Where there is no internal audit function, the audit committee should consider annually whether there is a need for it and make a recommendation to the board, and the reasons for the absence of such a function should be explained in the relevant section of the annual report.

---

1 As noted above, in this paper we refer to the actions of the audit committee. While boards often delegate day-to-day oversight to the audit committee (where there is one) final responsibility for internal audit rests with the board.
The audit committee reviews and approves internal audit’s remit, having regarded the complementary roles of the internal and external audit functions. It ensures that internal audit is free to work independently and objectively, i.e. free from the influence of those being audited. It ensures that internal audit has the necessary resources and access to information to enable it to fulfil its mandate, and is equipped to perform in accordance with appropriate professional standards for internal auditors (the Institute of Internal Auditors’ Code of Ethics and the International Standards for the Professional Practice of Internal Auditing). The committee also approves the appointment or termination of appointment of the Head of Internal Audit, and its chair should play a direct role in decisions concerning the Head of Internal Audit’s appraisal and remuneration.

In its review of the work of internal audit, the audit committee:

- Ensures that the Head of Internal Audit has direct access to the board chairman and to the audit committee, and is accountable to the audit committee;
- Ensures that internal audit is appropriately tasked and resourced, and has sufficient authority and standing to carry out its tasks effectively;
- Reviews and assesses the annual internal audit work plan;
- Receives a periodic report on the results of the internal auditors’ work;
- Reviews and monitors management’s responsiveness to the internal auditor’s findings and recommendations;
- Meets with the Head of Internal Audit at least once a year without the presence of management; and
- Monitors and assesses the quality and effectiveness of internal audit, and its role in the overall context of the company’s risk management system.
Internal audit has a key role in the corporate governance structure to assure on the effective management of risk:

- The board provides direction to senior management by setting the organisation's risk appetite. It also seeks to identify the principal risks facing the organisation. Thereafter, the board assures itself on an ongoing basis that senior management is responding appropriately to these risks.

- The board delegates to the CEO and senior management primary ownership and responsibility for operating risk management and control. It is management’s job to provide leadership and direction to the employees in respect of risk management, and to control the organisation’s overall risk-taking activities in relation to the agreed level of risk appetite.

To ensure the effectiveness of an organisation’s risk management framework, the board and senior management need to be able to rely on adequate line functions – including monitoring and assurance functions – within the organisation. The IIA and the IoD endorse the “Three Lines of Defence” model as a way of explaining the relationship between these functions and as a guide to how responsibilities should be divided.

- the first line of defence – functions that own and manage risk;
- the second line of defence – functions that oversee or specialise in risk management, compliance, etc. and
- the third line of defence – functions that provide independent assurance, above all internal audit.

Under the first line of defence, operational management has ownership, responsibility and accountability for directly assessing, controlling and mitigating risks.

The second line of defence consists of activities covered by several components of internal governance (compliance, risk management, quality, IT and other control departments). This line of defence monitors and facilitates the implementation of effective risk management practices by operational management and assists the risk owners in reporting adequate risk-related information up and down the organisation.

Internal audit forms the organisation’s third line of defence. An independent internal audit function will, through a risk-based approach to its work, provide assurance to the organisation’s board of directors and senior management (see Annex 5). This assurance will cover how effectively the organisation assesses and manages its risks and will include assurance on the effectiveness of the first and second lines of defence. It encompasses all elements of an institution’s risk management framework (from risk identification, risk assessment and response, to communication of risk-related information) and all categories of organisational objectives: strategic, ethical, operational, reporting and compliance.
Internal audit is uniquely positioned within the organisation to provide global assurance to the audit committee and senior management on the effectiveness of internal governance and risk processes. It is also well-placed to fulfil an advisory role on the coordination of assurance, effective ways of improving existing processes, and assisting management in implementing recommended improvements. In such a framework, internal audit is a cornerstone of an organisation’s corporate governance.

The use of the three lines of defence to understand the system of internal control and risk management should not be regarded as an automatic guarantee of success. All three lines need to work effectively with each other and with the audit committee in order to create the right conditions.

In some organisations the role of internal audit is combined with elements from the first two lines of defence. For example some internal audit functions are asked to play a part in facilitating risk management or managing the internal whistleblowing arrangements. Where that happens, boards need to be aware of potential conflicts of interest and ensure they take measures to safeguard the objectivity of internal audit. (See Annex 7 on whistleblowing and corporate governance).

---

**Internal audit effectiveness – Key issues for directors**

Before considering the detailed recommendations of this guidance, it is important to stress the four fundamental issues that should be considered by directors in order to ensure that internal audit maximises its contribution to good governance:

- Internal audit should have a functional reporting line to the board or one of its committees, making it independent of the executive, able to make objective judgements, and giving it the authority to conduct its work across the whole organisation without constraint. To work effectively it also needs a close relationship with the Chief Executive and should have access to management information going to the executive committee and board. (See Annex 5)

- Internal audit must be properly resourced, including ensuring a consistently high level of professionalism and quality based on the International Standards, plus appropriate knowledge, skills and experience.

- Internal audit should use a risk-based approach in developing and executing the internal audit plan in order to focus on the greatest threats to the organisation. (See Annex 5)

- Internal audit’s scope should be unrestricted, including all areas of risk – such as key corporate events, culture and ethics (see Annex 6), reputation, new products and the outcomes of processes.

The following recommendations for directors are consistent with the globally recognised International Standards for the Professional Practice of Internal Auditing (https://global.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx). (See Annex 3)
1. **Take responsibility for the provision of internal audit, including whether to have it and how it is provided.**

The introduction to this paper underlined the added value of an independent, professional internal audit function. For listed companies in the UK subject to the Corporate Governance Code, the presence of an internal audit function is required on a “comply or explain” basis. In addition, internal audit is compulsory for companies within the financial sector.

Audit committees should ensure that they have final responsibility for decisions that can affect the independence and objectivity of the internal audit function. In practice, this means that the internal audit’s functional reporting line should be to the audit committee.

More generally, in organisations that do not currently have an internal audit function (either in-house or out-sourced), the audit committee should regularly review the need for establishing one. As part of its management oversight role, and based on the underlying rationale submitted by senior management, the committee should either endorse or challenge any “go/no go” decision.

The probability and impact of organisational risks (including financial) and the complexity of the organisation, rather than simply its size, should be the decisive factors in the decision whether to establish an internal audit capability.

In some organisations, senior management and the audit committee may decide to opt for some form of outsourcing as a means of obtaining an internal audit capability. It is important, however, that in the case of full outsourcing, ultimate accountability for the function’s work cannot be delegated away from the company. Responsibility for internal audit should remain with the committee.

**Recommended practices:**

- The audit committee should ensure that it has final responsibility for decisions affecting internal audit’s independence and objectivity. These are outlined in the following sections.

- In organisations that have no internal audit function, the audit committee should periodically review the need for establishing such a function. Based on the underlying rationale submitted by senior management, the committee should then endorse or challenge this “go/no go” decision. This should be publicly disclosed (e.g., in the corporate governance statement) including a meaningful explanation of why this decision has been taken and how global assurance is to be obtained by the committee and senior management in its absence.

- In cases where an organisation’s management opts to fully outsource its internal audit function, the audit committee should oversee the entire outsourcing process, including ensuring that formal accountability for the appropriateness and quality of the outsourced work is not devolved and that there are no conflicts of interest.
2. Assess and approve the internal audit charter (terms of reference) and review regularly.

The internal audit charter is a formal document that defines the internal audit activity’s purpose, authority, and responsibility. The internal audit charter establishes internal audit’s position within the organisation, including the nature of the Head of Internal Audit’s (HIA) functional reporting relationship with the audit committee and senior management. It also authorises the internal audit department’s access to records, personnel, and physical locations relevant to the performance of engagements.

The internal audit charter also defines the scope of the internal audit activities. In order to optimise the contribution of internal audit to an effective governance structure, its scope of activity should not be confined to financial or administrative areas but preferably cover the full portfolio of organisational risks (strategic, operational, reporting, compliance) and include both assurance and consultancy activities.

It is important therefore to recognise that every internal audit charter is individual to the organisation, reflecting its unique structure, range of activities, geography and risks. As such the charter needs to be reviewed on a regular basis so that it is up-to-date and represents the full range of expectations of internal audit. It is essential that it keeps pace with the changes and emerging risks impacting the organisation, and the board’s risk appetite.

Although providing assurance that risks are understood and managed appropriately is internal audit’s core activity, internal audit may from time to time advise management and directors on issues of risk management, governance and internal control. This is however can raise questions about whether such a consultancy role compromises internal audit’s independence and objectivity. Where internal audit undertakes this role, audit committees should be aware of the risks and satisfy themselves that sufficient safeguards are in place so that the internal audit function is not compromised.

Final approval of the internal audit charter should always reside with the audit committee. It should be reviewed annually and updated if necessary to reflect any changes that may have taken place in the organisation. A sample internal audit charter is included in Annex 1 of this paper.

Recommended practices:

- The audit committee should review the internal audit charter to ensure that it allows the internal audit function to fully assume its responsibilities as a key assurance provider in respect of organisation-wide risk management and control. The audit committee should approve the internal audit charter annually, ensuring it fully reflects the role and expectations of internal audit as changes occur in the organisation.

“...In recent years we have been asked to provide consultancy services on a wider range of risks and business areas as the executive team has realised the value of our work. However, through the internal audit charter, our audit committee confirmed that our primary role is to serve the business as assurance providers; any consultancy work that internal audit carries out is secondary to its core focus. We have three criteria that need to be satisfied if we are going to carry out consultancy work. Firstly, the work we are being asked to do needs to materially impact the business. Secondly, we must have the skills within the team to be able to carry out the work. And thirdly, we must be able to have the time to do the work without jeopardising our activities in the core assurance programme.”
3. Ensure a close working relationship with the Head of Internal Audit, promoting effective formal and informal communication.

In order to ensure the independence of the internal audit function and the objectivity of its assessments, it is important that the internal audit function is not placed hierarchically under parts of the organisation that are themselves subject to internal audit scrutiny.

The HIA should have an open communication line with the audit committee, board and other directors, particularly the board chair. This is especially important when the HIA has reason to believe that senior management has exposed the organisation to a level of residual risk that may be unacceptable to the organisation on the basis of its agreed risk appetite. In such a case the HIA must be able to report the matter to the audit committee chair or board chair for evaluation.

Recommended practices:

- The board should ensure that the HIA is accountable to a non-executive board member, such as the chair of the audit committee.
- The HIA should enjoy direct and unrestricted access to the audit committee and the board chairs.
- The audit committee should conduct direct discussions with the HIA at least once a year without the presence of the CEO or other senior managers.
- The audit committee should be informed of any significant differences of opinion that arise between senior management and the HIA on significant risk and control issues.

“As the Senior Vice President and Director of Internal Audit, I report directly to the Chairman of the Board, thus ensuring Group Internal Audit’s independence within the organisation. All activities and processes can be audited. I meet with the Chairman of the Board on a monthly basis and work closely with the Chairman of the Audit Committee, having informal meetings approximately six times per year. I am regularly invited to attend audit committee meetings and discuss our activities. During these meetings, the audit committee members review the risk management and internal control system, approve the Internal Audit Plan, review a selection of high risk audit reports, and monitor the timely implementation of audit recommendations. In addition to my reporting relationship with the board and the audit committee, I also have a direct line of communication with the Group CEO and CFO with whom I have monthly meetings.”
4. Assess the resourcing of the internal audit function.

In order to be effective, the internal audit function must possess sufficient resources, both in terms of staff numbers and proficiency. The audit committee should devote significant thought and effort to the process of appointing the HIA. As the main contact point for the committee, this position must be staffed appropriately. Although the CEO may play a role in the HIA hiring process, the committee must ensure that it approves the functional profile and selection of the HIA. Furthermore, in view of the need to ensure the HIA’s independence and objectivity, the committee should also oversee the termination of the HIA’s appointment and seek to understand why a HIA has resigned.

The required capacity of the internal audit function should be based primarily on the risk-based audit plan. The HIA should demonstrate how individual audits link to principal risks, reporting the impact of any resource limitations implied by the plan to the CEO and audit committee. The committee should carefully consider the extent of risk coverage and monitor any proposal by the CEO to adjust the internal audit function’s capacity (as defined within the budgetary framework of the organisation). It should formally approve any list of principal risk areas which will not be covered by the internal audit process due to budgetary constraints.

The internal audit function should collectively possess, or have access to, the knowledge, skills, and other competencies needed to execute the plan. This will include a balanced set of technical skills which allow it to understand the types of risk faced by the organisation and to evaluate the effectiveness of associated risk responses. In addition to these technical skills, internal auditors should also demonstrate good interpersonal and communication skills (both oral and written).

The audit committee should ensure that an external assessment of the internal audit function is conducted at least once every five years – or more frequently if warranted (for example, where there has been significant change in personnel, scope or methodology) – by a qualified, independent reviewer or review team from outside the organisation (see point 5 below and annex 4 for more details).

The chair of the audit committee should be directly involved in the annual performance appraisal of the HIA.

Finally, the audit committee should make recommendations on the HIA’s remuneration package in order to ensure that:

- The level of his/her remuneration package is sufficient to attract the calibre of professional required and ensure a status within the organisation that allows him/her to carry out the assigned responsibilities.
- The variable performance part of his/her remuneration package avoids any real or perceived impairment of his/her independence and objectivity. In practice this will mean that remuneration is based on personal performance and the long term sustainability of the organisation rather than short term financial results.

Recommended practices:

- The audit committee, working with the CEO, should decide the functional profile of the HIA, and be involved directly in decisions in respect of his/her intended appointment/dismissal/resignation, appraisal and remuneration package. The committee should challenge the CEO on these issues in cases where the HIA’s independence or objectivity could be impaired.
- The audit committee should decide on any proposal to adjust the internal audit function’s capacity and formally approve any decision to omit principal risk areas from internal audit scrutiny due to resource constraints.
- The audit committee should periodically obtain assurance from the HIA that the internal audit function collectively possesses – or has access to – the required communication and technical skills to execute the internal audit plan effectively and to report engagement conclusions and recommendations adequately.
- The audit committee should consider the impact of skills gaps within internal audit and decide how to address them, bearing in mind options and costs in relation to the coverage of principal risks.
5. Monitor the quality of internal audit work, both in-house and external.

Monitoring the quality of the internal audit function, whether in-house or outsourced, is in the first instance the responsibility of the HIA. In order to fulfill this responsibility, the HIA should develop and maintain a quality assurance and improvement programme that covers all aspects of the internal audit function, in accordance with The IIA’s International Standards for the Professional Practice of Internal Auditing (the Standards). Such a programme should be mapped out and reviewed by the audit committee to ensure it has the necessary components to provide insight on the efficiency and effectiveness of the internal audit function and identify opportunities for improvement.

The quality assurance and improvement programme should include both internal and external assessments. Internal assessments should include ongoing performance monitoring of internal audit by means of direct supervision as well as periodic self-assessments. External assessments should be conducted at least once every five years – or more frequently if warranted – by an independent reviewer from outside the organisation qualified according to IIA Standards.

“ My team conducts an annual self-assessment, which comprises around 300 questions around internal audit positioning, resourcing, planning, methodology, reporting and quality. The team also produces a questionnaire – incorporating input from the audit committee – which is sent out annually by the chief executive (to preserve independence) via the intranet to the senior management group. Responses are not anonymised, so internal audit can follow up any comments with the individuals involved to improve the quality of its work. In addition, we try to get structured feedback from key auditees after every audit review on internal audit’s performance during the planning, fieldwork and reporting phases. The feedback considers – among other issues – auditor competence, communication and business understanding. ”

Recommended practices:

- The audit committee and the CEO should review the quality of the internal audit function on an annual basis.
- The audit committee should have full view of the quality assurance and improvement programme, including a timetable of key events, so that it knows when and how quality assessments will occur.
- The audit committee should periodically review whether an external assessment of the internal audit function should be conducted, although the minimum frequency should be every five years.
- The audit committee should review the qualifications and independence of the external reviewer or review team, including any potential conflicts of interest.
- The audit committee should effectively monitor the adequate and timely implementation of any corrective actions following the external quality assessment.
- Independent of, and in addition to the external quality review, the audit committee should assess the performance of the internal audit function, asking the following sorts of questions:
  - Is it looking at the right things?
  - Is it going deep enough to find out what the problems are and what are the root causes of those problems?
  - Is it making the committee aware quickly enough?
  - Are its conclusions credible?
  - Is it demonstrating independence and objectivity?
  - Is it offering advice or insight from experience?
  - Are its reports clear, concise and digestible?
  - Is it achieving what it sets out to do?
  - Can it repeat that achievement?
  - Could it be doing more useful work?
  - Does it use its resources and tools effectively?
  - Does it demonstrate effective planning, evidence collection, reporting and implementation?
6. Evaluate, approve and regularly review the risk-based annual internal audit plan.

The HIA is responsible for developing a risk-based plan on an annual basis to determine the priorities of internal audit activities, consistent with the organisation’s goals.

In this regard, the HIA should take into account the organisation’s risk management and internal control framework. The HIA should include the risk tolerance levels set by senior management and the board for the different activities or parts of the organisation and the assurance provided by management and specialist functions. The HIA should also define his/her own risk-based assessment criteria as the basis for the internal audit plan in consultation with senior management and the audit committee.

In practice the HIA should fully explain and justify the use of available internal audit resources, setting out a clear strategy that will enable the audit committee to form an overall opinion of the effectiveness of risk management and of the management of principal risks. The internal audit plan should provide a story board, showing the linkage between the organisation’s strategic objectives, principal risks, assurance over their management and planned internal audits, to enable the audit committee to judge whether they are receiving the depth and breadth of assurance that is needed. While there is no prescribed format and presentation of risk-based internal audit plans, the audit committee will need to be able to judge whether internal audit resources are applied appropriately to the issues that really matter to the organisation.

The final internal audit plan should be submitted to the audit committee for approval.

The audit plan should be dynamic, i.e. insight gained during the business year and/or evolutions in the organisation’s risk profile could result in an updating of the plan at relatively short notice. Such changes and the underlying rationale for those changes should be clearly communicated and coordinated with senior management and the audit committee.

Recommended practices:

- The audit committee and the CEO should provide input to the HIA in his/her drafting of a risk-based internal audit plan.
- The audit committee and the CEO should discuss the content of the audit plan with the HIA. Particular attention should be paid to:
  - The process used by the HIA to assess areas of significant risk to the organisation, which may affect the targeting of internal audit activities;
  - The extent of the internal audit universe, which will affect the potential breadth of internal audit’s activities within an organisation;
  - The extent to which both design and performance of internal control systems will be considered in the course of internal audit activity.
- After having reviewed and discussed the plan, and proposed changes as necessary, the audit committee should formally approve the internal audit plan.
- The audit committee and the CEO should discuss and approve any significant changes to the plan during the year proposed by the HIA.

"We continuously re-assesses our audit plan through a process known as “dynamic risk assessment”. This allows us adjust the annual audit plan to take account of emerging risks and to reprioritise assurance activities as required. We have a quarterly refresh to make sure that we are actually auditing the areas we need to, and whether there are areas where we should pull back from, or if we can rely on the work provided by other assurance providers. We simply need this flexibility built into our audit plan: we have already made dramatic changes to it within just the first quarter of the year and have switched our focus with regards to areas for review."
7. **Oversee the relationship between internal audit and centralised risk monitoring.**

Whilst the management of each part of an organisation should be responsible for managing risks in its own area of activity, this should take place within an integrated, holistic framework aimed at aligning organisation-wide objectives and strategy.

Many organisations have established a centralised risk management function for coordinating and developing risk management activities across the organisation. Whilst best practice for larger organisations may be to nominate a chief risk officer (CRO), smaller organisations may assign this responsibility to another senior executive.

The CRO (or equivalent) is responsible for monitoring overall risk management capabilities and resources, and for assisting operational managers to report relevant risk information up and across the organisation.

Specific responsibilities of a CRO (or equivalent) include:

- Establishing risk management policies, defining roles and responsibilities, and setting goals for implementation;
- Providing a framework for risk management in specific processes, functions or departments of the organisation;
- Promoting risk management competence throughout the organisation;
- Establishing a common risk management language (e.g. regarding risk categories and measures related to likelihood and impact);
- Facilitating managers’ development of risk reporting, and monitoring the reporting process;
- Reporting to the CEO and the board or relevant committee on progress and recommending action as needed.

In this role, the CRO (or equivalent) typically acts as a “second line of defence” risk monitoring function (see the Introduction for a description of the three lines of defence model).

To avoid overlaps and/or gaps in organisational risk monitoring, it is important that the internal audit function coordinates appropriately with the CRO (or similar function).

As a “third line” assurance function, internal audit should not only evaluate the effective design and proper functioning of risk and control systems implemented by (first line) operational management, but also the way in which second line of defence monitoring functions – such as centralised risk management – operate.

Internal Audit should also evaluate whether the governance structure, from the board downwards, provides for the effective management of risk across the organisation, including whether the full spectrum of risk is being appropriately considered and reported.

**Recommended practices:**

- The board, its committees and the CEO should ensure that there is appropriate task allocation and coordination between the internal audit function and second line of defence functions, such as risk management, financial controls and compliance.
- The audit committee should ensure that the internal audit function evaluates both first and second line of defence risk management activities as part of its internal audit plan and provides assurance on the effectiveness of the governance of risk, including how both lines of defence operate.
- Where the role of internal audit is combined with elements from the first two lines of defence, for example facilitating risk management or managing the internal whistleblowing arrangements, the audit committee must consider potential conflicts of interest and ensure it takes measures to safeguard the objectivity of internal audit. See Annex 7 and www.iia.org.uk/policy/policy-position-papers/risk-management-and-internal-audit/
8. Ensure the collective assurance roles of internal audit, other internal assurance providers and external audit, are coordinated and optimised.

External auditors provide assurance to the organisation's shareholders, board and senior management that the organisation's financial statements provide a ‘true and fair’ view of the organisation's financial performance and current financial position.

Given the specific scope and objectives of their mission, the risk information gathered by external auditors is typically limited to financial reporting risks, and does not include the way senior management and the board or board committees are managing/monitoring the organisation’s strategic, business and compliance risks.

These are areas in which the internal audit function can provide assurance to senior management, the board and audit committee (or other relevant governance committee). Audit committees should therefore ask for a simple mapping exercise to allow it to see who is providing assurance against each principal risk to consider and avoid duplication and gaps. This should begin with the second and third lines of defence as it will inform the risk-based internal audit planning process.

Whilst the objectives of external and internal audit activities are different, there may be some potential areas of overlap, particularly in the area of financial reporting. In particular, external audit may provide “management letter comments” in relation to internal control weaknesses noted in the course of their audit engagement.

Internal audit should consider these points in its audit planning process and may include follow up activity to ascertain the effectiveness of management’s corrective actions. Similarly, external audit may consider internal audit findings to inform their own work.

Internal audit also considers the effectiveness of other internal assurance providers, such as risk or IT managers, who may report separately to the board or its committees. The audit committee has a role to play in ensuring an adequate and effective coordination between internal and external audit activities and other assurance functions, avoiding duplication and optimising the use of each other’s work.

Recommended practices:

- The audit committee should ensure that there is open communication between internal and external auditors; they should oversee the manner in which the activities of the internal audit function and those of external audit optimise the use of each other’s work and avoid any risk of duplication.

- The audit committee should also ensure that the work of all internal and external assurance providers is coordinated and optimised to ensure that there are no significant gaps and that duplication of efforts is avoided.

We use, among other things, the results of the risk assessment performed by the external auditors in relation to their evaluation of financial reporting controls for building our own internal audit plan. We also meet with them on a regular basis to share audit plans and the results of our work. This way we mutually update our risk assessment information and aim at avoiding duplication of work. We also jointly participate in every audit committee meeting.
9. Assess internal audit findings and the breadth and depth of internal audit reports.

The audit committee should take an active role in clearly formalising their internal audit reporting and communication needs, including the required frequency of reporting, how internal audit opinions will be expressed and the grading of management actions / internal audit recommendations.

As a minimum requirement, internal audit reporting to the audit committee should include significant risk exposures, risk-taking that is outside risk tolerance levels and control issues identified by internal audit work, a progress report on the fulfilment of the internal audit plan and any issues of concern regarding the staffing and resources made available to the internal audit function. All of this should link back to the requirements set out with the internal audit charter.

Recommended practices:

• Based on a comprehensive overview, the audit committee should periodically consider and evaluate:
  – The most significant findings of internal audit during the latest audit period;
  – The progress and adequacy of implementation of internal audit recommendations by management;
  – Progress in executing the audit plan;
  – Issues of concern regarding the staffing and resources made available for the internal audit function;
  – The extent to which the internal audit charter fully reflects what internal audit does.

“Every month we have an activity report that goes to the executive directors, the executive heads and the audit committee members. We go through what we have completed, and what we are about to start, and explain whether we are behind schedule or if we need further resources. We also provide the audit committee with a list of recommendations and actions that have been completed, and I am upfront about highlighting which recommendations have not been implemented by management. Keeping the audit committee informed about our progress is key to building trust and earning respect.”
10. Monitor management implementation of internal audit recommendations.

The HIA should establish a follow-up process to ensure that internal audit recommendations have been implemented effectively. Where they are not, the HIA should confirm that senior management has fully understood and accepted responsibility for the risks of not taking action.

If the HIA believes that senior management, by not acting on an internal audit recommendation, has exposed the organisation to a level of residual risk that may not be acceptable to the board; he/she should discuss the matter in the first instance with senior management. If the management decision regarding residual risk is not explained to the satisfaction of the HIA, the HIA should report the matter to the audit committee.

Recommended practices:

- The audit committee should assess the progress of management actions to implement the audit recommendations, placing specific emphasis on major risk and control issues and implementation backlogs.
- The audit committee should discuss the causes of significant backlogs and, where these are present, follow-up with management.
- The audit committee should discuss with the HIA those cases where, by not acting on an internal audit recommendation, the HIA believes that senior management has exposed the organisation to a level of residual risk that may not be acceptable to the board.
Introduction

Internal Auditing is an independent and objective assurance and consulting activity that is guided by a philosophy of adding value to improve the operations of the <organisation>. It assists <organisation> in accomplishing its objectives by bringing a systematic and disciplined approach to evaluate and improve the effectiveness of the organisation’s risk management, control, and governance processes.

Organisation

The Head of Internal Audit will report functionally to the Board and administratively to the Chief Executive Officer. The Board will approve all decisions regarding the performance evaluation, appointment, or removal of the Head of Internal Audit as well as the Head of Internal Audit’s annual compensation and salary adjustment. The Head of Internal Audit will communicate and interact directly with the Board, including in executive sessions and between Board meetings as appropriate.

Independence and Objectivity

The internal audit activity will remain free from interference by any element in the organisation, including matters of audit selection, scope, procedures, frequency, timing, or report content to permit maintenance of a necessary independent and objective mental attitude.

The internal auditors will have no direct operational responsibility or authority over any of the activities audited. Accordingly, they will not implement internal controls, develop procedures, install systems, prepare records, or engage in any other activity that may impair internal auditor’s judgment.

The Head of Internal Audit will confirm to the board, at least annually, the organisational independence of the internal audit activity.

Role

The internal audit activity is established by the Board of Directors or oversight body (hereafter referred to as the Board). The internal audit activity’s responsibilities are defined by the Board as part of their oversight role.

Responsibility

The scope of internal auditing encompasses, but is not limited to, the examination and evaluation of the adequacy and effectiveness of the organisation’s governance, risk management, and internal control processes in relation to the organisation’s defined goals and objectives. Internal control objectives considered by internal audit include:

Professionalism

The internal audit activity will govern itself by adherence to The Institute of Internal Auditors’ mandatory guidance including the Definition of Internal Auditing, the Code of Ethics, and the International Standards for the Professional Practice of Internal Auditing (Standards). This mandatory guidance constitutes principles of the fundamental requirements for the professional practice of internal auditing and for evaluating the effectiveness of the internal audit activity’s performance.

The Institute of Internal Auditors’ Practice Advisories, Practice Guides, and Position Papers will also be adhered to as applicable to guide operations. In addition, the internal audit activity will adhere to <organisation> relevant policies and procedures and the internal audit activity’s standard operating procedures manual.

Authority

The internal audit activity, with strict accountability for confidentiality and safeguarding records and information, is authorised to have full, free, and unrestricted access to any and all of the organisation’s records, physical properties, and personnel pertinent to carrying out any engagement. All employees are requested to assist the internal audit activity in fulfilling its roles and responsibilities. The internal audit activity will also have free and unrestricted access to the Board.
• Consistency of operations or programs with established objectives and goals and effective performance;
• Effectiveness and efficiency of operations and employment of resources;
• Compliance with significant policies, plans, procedures, laws, and regulations;
• Reliability and integrity of management and financial information processes, including the means to identify, measure, classify, and report such information;
• Safeguarding of assets.

Internal Audit is responsible for evaluating all processes (‘audit universe’) of the entity including governance processes and risk management processes. It also assists the Audit Committee in evaluating the quality of performance of external auditors and maintains proper degree of coordination with internal audit.

Internal audit may perform consulting and advisory services related to governance, risk management and control as appropriate for the organisation. It may also evaluate specific operations at the request of the Board or management, as appropriate.

Based on its activity, Internal audit is responsible for reporting significant risk exposures and control issues identified to the Board and to Senior Management, including fraud risks, governance issues, and other matters needed or requested by the Board.

**Internal Audit Plan**

At least annually, the Head of Internal Audit will submit to the Board an internal audit plan for review and approval, including risk assessment criteria. The internal audit plan will include timing as well as budget and resource requirements for the next fiscal/calendar year. The Head of Internal Audit will communicate the impact of resource limitations and significant interim changes to senior management and the Board.

The internal audit plan will be developed based on a prioritisation of the audit universe using a risk-based methodology, including input of senior management and the board. Prior to submission to the Board for approval, the plan may be discussed with appropriate senior management. Any significant deviation from the approved internal audit plan will be communicated through the periodic activity reporting process.

**Reporting and Monitoring**

A report will be prepared and issued by the Head of Internal Audit or designee following the conclusion of each internal audit engagement and will be distributed as appropriate. Internal audit results will also be communicated to the Board.

The internal audit report may include management’s response and corrective action taken or to be taken in regard to the specific findings and recommendations. Management’s response, whether included within the original audit report or provided thereafter (e.g. within thirty days) by management of the audited area should include a timetable for anticipated completion of action to be taken and an explanation for any corrective action that will not be implemented.

The internal audit activity will be responsible for appropriate follow-up on engagement findings and recommendations. All significant findings will remain in an open issues file until cleared.

**Periodic Assessment**

The Head of Internal Audit is responsible also for providing periodically a self-assessment on the internal audit activity as regards its consistency with the Audit Charter (purpose, authority, responsibility) and performance relative to its Plan.

In addition, the Head of Internal Audit will communicate to senior management and the Board on the internal audit activity’s quality assurance and improvement program, including results of ongoing internal assessments and external assessments conducted at least every five years.

Internal Audit Activity charter

Approved this .............. day of .................., ..................

.....................................................................................

Head of Internal Audit   Chief Executive Officer

.....................................................................................

Chairman of the Board of Directors
Chairman of the Audit Committee

(Source: Institute of Internal Auditors)
Annex 2
Sample audit committee charter

Purpose
To assist the board of directors in fulfilling its oversight responsibilities for the financial reporting process, the system of internal control, the audit process, and the company’s process for monitoring compliance with laws and regulations and the code of conduct.

Authority
The audit committee has authority to conduct or authorize investigations into any matters within its scope of responsibility. It is empowered to:

• Appoint, compensate, and oversee the work of any registered public accounting firm employed by the organisation;
• Resolve any disagreements between management and the auditor regarding financial reporting;
• Pre-approve all auditing and non-audit services;
• Retain independent counsel, accountants, or others to advise the committee or assist in the conduct of an investigation;
• Seek any information it requires from employees—of whom are directed to cooperate with the committee’s requests—or external parties;
• Meet with company officers, external auditors, or outside counsel, as necessary.

Composition
The audit committee will consist of at least three and no more than six members of the board of directors. The board or its nominating committee will appoint committee members and the committee chair.

Each committee member will be both independent and financially literate. At least one member shall be designated as the «financial expert», as defined by applicable legislation and regulation.

Meetings
The committee will meet at least four times a year, with authority to convene additional meetings, as circumstances require. All committee members are expected to attend each meeting, in person or via tele- or video-conference.

The committee will invite members of management, auditors or others to attend meetings and provide pertinent information, as necessary. It will hold private meetings with auditors (see below) and executive sessions. Meeting agendas will be prepared and provided in advance to members, along with appropriate briefing materials. Minutes will be prepared.

Responsibilities
The committee will carry out the following responsibilities:

Financial Statements
• Review significant accounting and reporting issues, including complex or unusual transactions and highly judgmental areas, and recent professional and regulatory pronouncements, and understand their impact on the financial statements;
• Review with management and the external auditors the results of the audit, including any difficulties encountered;
• Review the annual financial statements, and consider whether they are complete, consistent with information known to committee members, and reflect appropriate accounting principles;
• Review other sections of the annual report and related regulatory filings before release and consider the accuracy and completeness of the information;
• Review with management and the external auditors all matters required to be communicated to the committee under generally accepted auditing Standards;
• Understand how management develops interim financial information, and the nature and extent of internal and external auditor involvement;
• Review interim financial reports with management and the external auditors before filing with regulators, and consider whether they are complete and consistent with the information known to committee members.

Internal Control
• Consider the effectiveness of the company’s internal control system, including information technology security and control.
• Understand the scope of internal and external auditors’ review of internal control over financial reporting, and obtain reports on significant findings and recommendations, together with management’s responses.
Internal Audit

- Review with management and the Head of Internal Audit the internal audit charter, activities, staffing, and organisational structure of the internal audit function.
- Have final authority to review and approve the annual audit plan and all major changes to it, and ensure there are no unjustified restrictions or limitations placed on it.
- Have final authority to review and approve the annual internal audit budget.
- Have final authority to review and approve the appointment, replacement, or dismissal of the Head of Internal Audit.
- At least once per year, review the performance of the Head of Internal Audit and approve the annual salary adjustment and compensation package.
- Review the effectiveness of the internal audit function, including compliance with The Institute of Internal Auditors’ International Professional Practices Framework for Internal Auditing consisting of the Definition of Internal Auditing, Code of Ethics and the Standards.
- On a regular basis, meet separately with the Head of Internal Audit to discuss any matters that the committee or internal audit believes should be discussed privately.

External Audit

- Review the external auditors’ proposed audit scope and approach, including coordination of audit effort with internal audit.
- Review the performance of the external auditors, and exercise final approval on the appointment or discharge of the auditors.
- Review and confirm the independence of the external auditors by obtaining statements from the auditors on relationships between the auditors and the company, including non-audit services, and discussing the relationships with the auditors.
- On a regular basis, meet separately with the external auditors to discuss any matters that the committee or auditors believe should be discussed privately.

Compliance

- Review the effectiveness of the system for monitoring compliance with laws and regulations and the results of management’s investigation and follow-up (including disciplinary action) of any instances of noncompliance.
- Review the findings of any examinations by regulatory agencies, and any auditor
- Review the process for communicating the code of conduct to company personnel, and for monitoring compliance therewith.
- Obtain regular updates from management and company legal counsel regarding compliance matters.

Reporting Responsibilities

- Regularly report to the board of directors about committee activities, issues, and related recommendations.
- Provide an open avenue of communication between internal audit, the external auditors, and the board of directors.
- Report annually to the shareholders, describing the committee’s composition, responsibilities and how they were discharged, and any other information required by rule, including approval of non-audit services.
- Review any other reports the company issues that relate to committee responsibilities.

Other Responsibilities

- Perform other activities related to this charter as requested by the board of directors.
- Institute and oversee special investigations as needed.
- Review and assess the adequacy of the committee charter annually, requesting board approval for proposed changes, and ensure appropriate disclosure as may be required by law or regulation.
- Confirm annually that all responsibilities outlined in this charter have been carried out.
- Evaluate the committee’s and individual members’ performance on a regular basis.

Internal Audit Activity charter

Approved this ................. day of ................, .............

............................................................................................

Chairman of the Board of Directors
Chairman of the Audit Committee

(Source: Institute of Internal Auditors)
Ensuring that the internal audit function understands and can meet the board’s expectations is critical. The relationship between the audit committee chair and HIA is key to this. The recruitment, remuneration, appraisal and dismissal of the HIA are therefore important responsibilities of the audit committee. Here are some considerations for audit committee chairs:

**Personal integrity**

The HIA must demonstrate a commitment to the highest moral and ethical standards and be willing to raise challenging questions. The HIA should be able to “stick to their guns” when necessary and have the strength of character to remain independent.

**Flexibility**

But they must also be willing to take wider business and commercial issues into account. They must advocate the value of control without becoming a “control freak”. The HIA must demonstrate flexibility, realism and practicality in order to build trust, confidence and credibility but without compromising objectivity.

**Diplomacy**

Resolving conflict, rather than provoking them is an important trait of the HIA. Internal audit is independent and objective, but it has to work with the organisation rather than against it.

**Skills and experience**

The knowledge needed for internal audit embraces the whole range of risks facing the organisation, now and in the future – financial, IT security, supply chains, organisational culture, legal and regulatory compliance, etc. A declining proportion of internal auditors holds accounting qualifications, with internal auditors coming from an expanding range of specialist backgrounds including engineers, scientists, analysts etc. Internal audit qualifications supplement this expertise by developing the technical internal audit knowledge and skills needed. Many HIAs will need to operate across the extensive range of risks their organisation faces and manage a diverse team. Some of the most effective HIAs move between industries and sectors, without extensive direct experience of the organisation’s particular business/operations. However an understanding of the organisation’s operational drivers is likely to be important, alongside a solid grounding in the techniques of internal audit gained both through practical experience and/or training/qualifications.

**Technical proficiency**

HIAs must be able to analyse business processes and associated controls; and they must be able to form a thorough understanding of the organisation, its strategic objectives and how it operates day to day. They must also be able to identify the assurance that management and the board require to support decision-making.

**Communication**

HIAs must be persuasive and clear communicators, able to cultivate relationships with management and negotiate effectively to win support without compromising their independence and objectivity. Informal communication skills, in particular in the key relationship between the HIA and audit committee chair, are increasingly important as attention focuses on more subjective, “gut feel” issues like culture. Effective HIAs are capable of alternating at will between attending to precise details and stepping back to encompass the wider more strategic point of view and can communicate with staff at all levels of the organisation.

**Standards and ethics**

The effective HIA is committed to the highest professional and ethical standards. These are set out in the Institute of Internal Auditors’ Code of Ethics and International Standards for the Professional Practice of Internal Auditing. These documents provide guidance on many of the issues highlighted in this report.

For more information about the IIA Code of Ethics and Standards, see https://global.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx
Annex 4
Evaluating the effectiveness of internal audit

How good is your internal audit function? Does it add value to your organisation and to you as a member of the audit committee? What is it that makes an internal audit function effective? And does your internal audit function have what it takes? Every audit committee must be able to ask these fundamental questions and to evaluate the answers.

Key questions for evaluating the effectiveness of internal audit

Purpose, authority and responsibility

• Has the purpose, authority and responsibility of the internal audit function been formally defined in a charter and approved by the audit committee?
• Does the charter reflect the full range of internal audit responsibilities, including those around change and project management?
• Are there any areas of the organisation not covered by internal audit?
• Does the charter define the nature of consulting and other services, such as direct involvement in fraud investigation and whistleblowing, that the internal audit function may perform without compromising the value of its assurance role?

Independence

• Does the head of internal audit report directly to the audit committee on its plans and findings?
• Is the HIA free from any operational responsibility that might impair independence and objectivity?
• Does the head of internal audit have direct access to the chair of the board?

Objectivity

• Have any members of the internal audit function given assurance on business areas or projects for which they were previously responsible?
• Have the internal audit function’s consulting activities in any other way detracted from its assurance role?
• Have criteria been established to enable a review of proposed diversion of resources from planned audit reviews?
• Is the remuneration structure of internal audit linked to performance in its work and decoupled from incentives relating to profit or turnover?

Proficiency

• Does the internal audit function have the appropriate technical expertise, qualifications and experience to provide assurance in all areas of the business?
• If internal audit staff lack the knowledge, skills, or other competencies needed to perform an audit, does the head of internal audit obtain competent advice and assistance from elsewhere?
• Is the internal audit function capable of identifying the indicators of fraud?

Due professional care

• Have internal audit assignments considered all relevant business issues and risks?
• Has the internal audit function considered adequately the monetary and operational cost of control and assurance and balanced it against the benefits?
• Does the internal audit function exhibit an understanding of the organisation and its key processes and related risks?
• Have there been any significant control breakdowns or surprises in areas that have been reviewed by the internal audit function?
Quality assurance and improvement in the internal audit function

- Does the internal audit function have clear systems for measuring its effectiveness and the value it delivers?
- Does the internal audit function strive to provide a continuously improving service?
- Does the internal audit function show that it responds to feedback?
- Is the internal audit function viewed as a valued asset within the organisation?
- Is an independent assessment of the internal audit function performed at least every five years?
- Is the performance of the internal audit function benchmarked against industry best practice?

Providing assurance and generating improvements in the organisation

- Does the internal audit function perform its work in accordance with the IIA’s Code of Ethics and the International Standards for the Professional Practice of internal Auditing? For organisations in the Financial Services sector, has the IIA’s Code, “Effective Internal Audit in the Financial Services sector (published in July 2013) been adopted?
- Does internal audit have sufficient standing and authority in the organisation and unlimited scope to allow it to audit any and every aspect of activity?
- Is the work of the internal audit function risk-based (see Annex 5)?
- Does the internal audit function include all risk areas – financial, operational, technological and behavioural – in its work programme?
- Can the internal audit function respond quickly to changes within the organisation?
- Does internal audit have the necessary resources and access to information to enable it to fulfil its mandate?
- Do internal audit reports contain an opinion on the adequacy of control?
- Is the internal audit function adept at communicating the results of its findings, building support and securing agreed outcomes?
- Does the internal audit function ask powerful questions that stimulate debate and improvements in key risk areas?
- Are significant control issues raised at an appropriate level in the organisation?
- Does management feel that recommendations made by the internal audit function are useful, realistic, forward looking and meet their needs?
Risk based internal auditing (RBIA) is a methodology that links internal audit to an organisation’s principal risks and risk appetite, relevant to its strategic objectives. RBIA allows internal audit to provide assurance to the board that risk management processes are managing risks effectively in relation to the risk appetite.

RBIA

- Is the most effective way for internal audit to provide directors with the independent and objective assurance that they need;
- Directs scarce internal audit resources to assessing the management of the highest risks: those that pose a serious threat to an organisation;
- Highlights risks that are over-controlled and consuming unnecessary resources;
- Helps to define how much internal audit resource the organisation needs to provide the assurances its board seeks;
- Gives a clear warning if an organisation’s risk management framework is not effective;
- Helps the audit committee question and challenge management more effectively on its perception and management of risk;
- Provides assurance over all parts of the risk management process. The audit plan may contain audits not carried out by auditors before, for example, on covering risks affecting public relations, supply chain management and treasury;
- Is acknowledged by many regulators as one of the most effective risk assurance methodologies.

Reinforces the responsibility of management for risk management at every stage and helps the organisation to grow stronger and more able to take on and manage risks. **RBIA is an ongoing process that comprises three distinct stages.**

**Annex 5**

**What is Risk-based internal auditing?**

RBIA starts by assessing the risk maturity of the organisation according to the following criteria:

- **Risk Naive**
  - No formal approach developed for risk management

- **Risk Aware**
  - Scattered silo based approach to risk management

- **Risk Defined**
  - Strategy and policies in place and communicated. Risk appetite defined

- **Risk Managed**
  - Enterprise wide approach to risk management developed and communicated

To benefit from RBIA, an organisation has to have a high level of risk maturity because internal audit can provide assurance on the risk management framework only if it exists.

**2. Developing the periodic audit plan**

The next step is to develop the periodic audit plan, which starts from the organisation’s risk register, takes account of internal audit’s own view of strategic risk, and responds to the directors’ requirement for objective assurance. The audit plan will include a mixture of services. There will be assignments designed to give assurance on the management of risk. There may also be consulting assignments to facilitate the improvement of the risk management framework.
3. Undertaking individual audit assignments

RBIA also provides a methodology for individual audits. During these assignments internal audit will gather the evidence it needs to provide assurance to directors and audit committee members on the risk management framework, on the management of individual risks and on the reliability of management reporting. Under RBIA, internal audit will report in language and formats that are consistent with those of risk management reports. The results of each internal audit assignment may require management to revise or amend the risk register, or internal audit to revise its assessment of the overall risk maturity.

Using RBIA enables internal audit to provide assurances on:

- The design of risk management processes;
- How well the processes are working;
- The effectiveness of responses to key risks, including internal controls;
- The reliability of management assurances;
- The completeness, accuracy and appropriateness of management’s classification and reporting of risks.

RBIA does not mean that internal audit manages an organisation’s risks: that is the responsibility of management. Nor does it mean that internal audit simply takes into account in each audit the risks that management identifies. Instead, RBIA is a strategic initiative that ties all internal audit work into management’s own assessment of risk, at the same time as reinforcing management’s responsibilities.
Annex 6
The governance of culture and the role of internal audit

Following a series of scandals, fundamental changes in organisational culture are being called for across many sectors. How organisations, and individuals within them, behave has become a matter of public concern. Poor organisational culture has been identified as the root cause of many scandals, which have resulted in great cost to individuals, organisations and even countries.

The FRC Corporate Governance Code gives a key role to the board in establishing culture, values and ethics, considering, among other things, the culture it wishes to embed in the company and whether this has been achieved. It is not sufficient for the board simply to set the desired values. It also needs to ensure they:

- are communicated by management;
- incentivise the desired behaviours and sanction inappropriate behaviour, and;
- assess whether the desired values and behaviours have become embedded at all levels.

The audit committee is normally charged with giving the board assurances on the quality of all the above processes. The ownership of such programmes to promote the desired culture must lie with the executive. Internal audit’s main role is to analyse to what extent processes (such as performance management and remuneration), actions (such as decision making) and tone at the top are in line with the values, ethics, risk appetite and policies of the organisation. They can therefore help audit committees judge whether measures put in place to influence culture and thus behaviour are actually working. Internal audit can also play an advisory role on processes and controls in cultural change programmes to ensure that they can be measured and judgements made. It is important that audit committees engage with internal audit on culture from the start, so that policies and processes can be developed that build in the need for assurance.

The IIA has produced a report showing the role internal audit is playing to support the audit committee on culture. HIAs are taking two main approaches to auditing cultural indicators.

1. The first is to incorporate culture into each audit, through techniques like root cause analysis, identifying why issues occur and how they can be the drivers for wrong behaviours, and then to join the dots across individual audits.

This takes them beyond focussing on processes and controls and requires them to combine hard data with gut feel. They also need to have a different type of dialogue with the audit committee chair and CEO, using more subjective judgements. Some say that this is what any good internal audit has been doing all along but only now is it being badged as culture. Others see this as a new departure.

2. The second approach is auditing cultural indicators across the organisation through auditing personal behaviours as a proxy for culture. Here the key question is how best to gather evidence to show that culture and values are at the heart of every business decision and are being incorporated at every level in recruitment, training, performance management and reward arrangements.

This second approach requires internal audit to engage in new ‘soft’ techniques and work more closely with other functions, such as HR. This approach is less common, but, over time, may be adopted more widely in addition to the first approach if deemed helpful to the organisation and its circumstances.

Challenges and enablers

In order to harness internal audit’s support of boards in relation to culture most effectively, audit committees need to be aware of the enablers and challenges that internal audit faces.

Challenges – issues facing internal audit in carrying out work on culture

- Organisational culture is often underpinned by how a statement of values is translated into concrete actions. The key question is how to gather evidence and demonstrate that this is happening and that the desired values are being lived at every level.

- Limitations of surveys and interviews. While culture may be tracked and measured in visible ways, the very instruments which exist to do this e.g. staff surveys, provide only indirect observations of behaviour at best. Employee surveys may be skewed if not underpinned by a culture of being able to speak openly and honestly.
• Skills and training:
  – Internal audit will need to develop more qualitative methods such as surveys and interviews, or co-source in this area. Surveys need to be properly constructed, administered, analysed and interpreted to identify weaknesses.
  – The use of gut feel can play an important part in the audit of culture. Internal auditors who are used to reporting hard facts will need to develop soft skills to obtain a picture of what underlies culture. They will need to employ root cause analysis i.e. going beyond processes and controls to look at behaviours that influence decisions.
  – Senior internal auditors will require new communication and relationship skills to enable them to conduct more subjective and informal discussions with NEDs and executives about cultural issues.

• Reporting. The internal audit team needs to develop and report results in partnership with those accountable, using appropriate means. This can be problematic:
  – Managers may agree with the weaknesses verbally but get defensive when they see them written in an audit report. This in turn may make it more difficult to evaluate cultural aspects in the future.
  – It can be difficult to express weaknesses in writing which could then be open to misinterpretation leading to superiors making unfair judgements on the manager in question.

• Internal audit is part of the culture itself. Despite being independent and objective, internal audit, without realising it, may have adopted the same cultural values and ethics as the rest of the organisation. Internal audit needs to distance itself from cultural drivers, such as remuneration.

Enablers – crucial foundations necessary for the audit of culture

• Organisational culture needs to have been analysed, properly defined and disseminated by the board/senior management i.e. what is required behaviour in the organisation has been made explicit.
• Appetite and support from the top of the organisation.
• Internal audit being given a clear mandate.
• Writing the mandate into the audit charter.
• A relationship of trust between the audit committee chair and HIA that allows informal discussion about subjective judgements (gut feel) on culture.
• Position, treatment and regard for internal audit, and non-adversarial relationships with their clients.
• The ability for clients to report or respond to surveys confidentially.
• A good level of risk maturity in the organisation.
• The development in internal auditors of a challenge mentality arising from the requirement (in the International Standards for internal audit) for objectivity and independence. This gives them impartiality, detachment and a helicopter view of events, allowing them to act as participant observers, taking part in their organisation but able to observe, analyse and report on cultural norms.

The Institute is also providing its member internal auditors with technical guidance to help equip internal audit to play its proper role in the assessment of organisational culture. It contains full details on the examples of the different approaches to auditing culture and examples of how this is starting to be done. This guidance is also available to non-members for a charge.²

² www.iio.org.uk/resources/ethics,-values-and-culture/organisational-culture/
Whistleblowing is an essential safety valve, an important element in a healthy corporate culture, and should be part of the internal control environment.

For listed companies, the UK Corporate Governance Code states that boards should ensure these procedures are properly planned and properly implemented (reference Section C.3.5).

Whistleblowing procedures should encourage individuals to disclose concerns using appropriate channels before these concerns become a serious problem, thus avoiding reputational damage through negative publicity, regulatory investigation, fines and/or compensation.

Boards need to consider the effectiveness of whistleblowing policies and procedures on a regular basis as part of their oversight of the system of internal control.

Internal audit can play a vital role in supporting boards in this area.

What is whistleblowing?

Whistleblowing is when an employee, contractor or supplier goes outside the normal management channels to report suspected wrongdoing at work, i.e. speaking out in a confidential manner. This can be done via internal processes set up by the organisation (internal whistleblowing) or to an external body such as a regulator (external whistleblowing). While public disclosure to the media can also be perceived as whistleblowing the IIA report focuses on formally prescribed channels.

Key issues for Audit Committees

While the responsibility for establishing and operating effective internal whistleblowing procedures lies with the executive, boards should maintain oversight and require independent assurance that the organisation’s whistleblowing policies and procedures are effective in achieving the appropriate outcomes.

Given the potential conflicts of interest, the executive will need to devolve the day-to-day running of the process to a function that is considered to be independent. Internal audit’s independence from the executive and objectivity give it the potential to be involved in whistleblowing arrangements, e.g. in a triage role, as a channel of communication or carrying out investigations.

Internal audit cannot give assurance to the board on effectiveness if it is playing an integral part in the process of internal whistleblowing in the organisation. Audit Committee Chairs should discuss the issue with their Head of Internal Audit to ensure that internal audit’s involvement in whistleblowing does not undermine its ability to carry out its prime assurance functions.

Where internal audit is involved in the procedures for whistleblowing the board should ensure:

- There is a separate, independent mechanism to provide assurance on the effectiveness of the whistleblowing procedures
- Internal audit’s main functions and wider assurance roles are not compromised
- Internal audit is properly resourced in terms of staffing and skills

Where internal audit is not playing a direct whistleblowing role it should provide assurance on the effectiveness of the system and procedures to the board. It also should have the right to be informed of all whistleblowing reports so that it can consider what impact they have on its overall opinion to the board concerning risk management and internal control in the organisation.
How is internal audit involved in whistleblowing? – Main findings from the IIA’s survey of Heads of Internal Audit

- 41% of HIAs have day-to-day responsibility for their organisation’s whistleblowing arrangements
- 31% lack confidence in their organisation’s whistleblowing arrangements
- 57% of staff members named in policies have not received any training
- 59% may include personal complaints or grievances in their whistleblowing report

The IIA has produced a report on whistleblowing (http://www.iia.org.uk/policy/whistleblowing-report/). Our policy approach informs boards, executives and Heads of Internal Audit in establishing or developing internal audit’s role to ensure that whistleblowing procedures are effective.
About the Chartered Institute of Internal Auditors

First established in 1948, the Chartered Institute of Internal Auditors (IIA) obtained its Royal Charter in 2010. It is the only professional body dedicated exclusively to training, supporting and representing internal auditors in the UK and Ireland. It has over 8,500 members in all sectors of the economy including private companies, government departments, utilities, voluntary sector organisations, local authorities and public service organisations such as the National Health Service.

Over 2,000 members of the institute are Chartered Internal Auditors and have earned the designation CMIIA. Over 800 of our members hold the position of head of internal audit and the majority of FTSE 100 companies are represented amongst the institute’s membership.

Members of the Chartered Institute of Internal Auditors are part of a global network of over 185,000 members in 190 countries. All members across the globe work to the same International Standards and Code of Ethics.

More information on the Institute is available at www.iia.org.uk