Chartered Institute of Internal Auditors

01 February 2023

Ten ways to get the most from internal audit

Chartered Institute of Internal Auditors

Here are ten essential actions for boards to ensure that their organisation maximises the value of its internal audit and gains maximum protection and assurance from its activities.

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

These are described in more detail below.

---

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 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 for boards

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 an 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.

See our sample internal audit charter

Recommended practices for boards

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 organisationwide 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.

A head of internal audit said ...

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.

1. The work we are being asked to do needs to materially impact the business.

2. We must have the skills within the team to be able to carry out the work.

3. 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 for boards

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.

A director of internal audit said ...

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 with 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.

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:

1. 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.

2. 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 for boards

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 and the CEO should obtain advice from the HIA on the impact of resource limitations on the internal audit plan.

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 fulfil 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.

Recommended practices for boards

1. The audit committee and the CEO should review the quality of the internal audit function on an annual basis.
2. 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.
3. 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.
4. The audit committee should review the qualifications and independence of the external reviewer or review team, including any potential conflicts of interest.
5. The audit committee should ensure that it is informed in a timely manner of the results and related actions for improvement of the internal audit assessment process and determine the required frequency for the internal assessments.
6. The audit committee should effectively monitor the adequate and timely implementation of any corrective actions following the external quality assessment.
7. 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:

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?

A head of internal audit said ...

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 otherissues - auditor competence, communication and business understanding.

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 riskbased 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 for boards

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.

A head of internal audit said ...

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:

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.

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 for boards

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.

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 for boards

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.

A head of internal audit said ...

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 for boards

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.

A head of internal audit said ...

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 for boards

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.

A head of internal audit said ...

We are very public about saying which recommendations and actions are overdue and we chase this with the management teams that are responsible for them.

We keep the audit committee in the loop. Every quarter I take a report to the audit committee that also provides an update of where we are and a performance overview.

The audit committee wants to know that we are independent and that we can stand up to management and provide an independent challenge.

Next: How internal audit works with the audit committee