Deloitte.

The Deloitte Academy
January 2020

Governance in brief

IIA raises the bar on internal audit

Headlines

- The Institute of Internal Auditors is seeking to reinforce the role of the internal audit profession as a cornerstone of good corporate governance and to enhance its impact through the publication of this Internal Audit Code of Practice.
- This builds on earlier work developing a similar Code of Practice for financial services firms.
- The Code aims to be regarded as a benchmark of good practice against which organisations can assess their internal audit function. The code should be applied proportionately based on an organisation's size, risk profile, internal organisation and the nature, scope and complexity of their operations.
- This is a far reaching Code and will raise the bar for many organisations, should they wish to comply with the Code. The following recommendations are particularly far reaching, recommending that internal audit:
  - there should be no aspect of the organisation which internal audit should be restricted from looking at when delivering its mandate;
  - assesses whether the information presented to the board and executive management fairly represents the benefits, risks and assumptions associated with the strategy and corresponding business model;
  - assesses whether risk appetite is embedded within the activities, limits and reporting of the organisation;
  - includes within its scope the risk and control culture of the organisation;
  - at least annually provides the audit committee with an assessment of the overall effectiveness of the governance, and risk and control framework of the organisation, and its conclusions on whether the organisation's risk appetite is being adhered to; and
  - has the right to attend and observe all or part of executive committee meetings.
- The code is intended to be applied by all organisations in the private and third sectors with an internal audit function and an audit committee of independent non-executive directors or their equivalent. While it may prove useful for internal audit in the public sector, it is not drafted with the public sector specifically in mind.

The Code of Practice

The recommendations contained within the Code are principles-based, rather than establishing detailed rules. They should be applied proportionately, dependent on the size and complexity of the organisation.

The Internal Audit Code of Practice includes the following elements:

Role and mandate of internal audit	• The primary role of internal audit should be to help the board and executive management to protect the assets, reputation and sustainability of the organisation. • Internal audit should be assessing whether all significant risks are identified and appropriately reported by management to the board and executive management as well as assessing whether they are adequately controlled. It should also challenge executive management to improve the effectiveness of governance, risk management and internal controls. The role of internal audit should be articulated in an internal audit charter, which should be publicly available. • The board, its committees and executive management should set the right 'tone at the top' to ensure support for, and acceptance of, internal audit at all levels of the organisation.
Scope and priorities of internal audit	• Internal audit's scope should be unrestricted – its scope should include information presented to the board and its committees. • Internal audit should form its own judgement on how best to segment the audit universe given the structure and risk profile of the organisation. • In setting its scope, internal audit should take into account business strategy and should form an independent view of whether the key risks to the organisation have been identified, including emerging and systemic risks, and assess how effectively these risks are being managed. • Judgement should be exercised in relation to which areas should be covered in the audit plan, and on the frequency and method of audit cycle coverage and this should be subject to approval by the audit committee. • Internal audit plans, and material changes to internal audit plans, should be approved by the audit committee. • The internal audit plan should have the flexibility to deal with unplanned events to allow emerging risks to be prioritised. Changes to the audit plan should be considered in light of internal audits ongoing assessment of risk.

Scope and priorities of internal audit (continued)	As a minimum, internal audit should include within its scope the following areas: • internal governance - the design and operating effectiveness of the internal governance structures and processes of the organisation. • the information presented to the board and executive management for strategic and operational decision-making - whether the information presented to the board and executive management fairly represents the benefits, risks and assumptions associated with the viability of the strategy and corresponding business model. • the setting of, and adherence to, the risks the entity is willing to accept (risk appetite) – it should assess whether risk appetite is embedded within the activities, limits and reporting of the organisation; and report annually to the audit committee on whether the organisation's risk appetite is being adhered to. • the risk and control culture of the organisation - assessing whether the processes (e.g. appraisal and remuneration), actions (e.g. decision-making), 'tone at the top' and observed behaviours across the organisation are in line with the espoused values, ethics, risk appetite and policies of the organisation. • key corporate events – internal audit should decide on a timely basis if these events (business process change, new products and services, outsourcing decisions and acquisitions/divestments etc) are sufficiently high risk to warrant involvement. Internal audit should evaluate whether the key risks are being adequately addressed (including by other forms of assurance, e.g., due diligence) and reported. • outcomes of processes – evaluating the design and operating effectiveness of the organisation's policies and processes considering the actual outcomes which result from their application, assessed against the espoused values, ethics, risk appetite and policies of the organisation.
Reporting results	Internal audit's reporting to the audit and/or any other board committees should include: • a focus on significant control weaknesses and breakdowns together with a robust root-cause analysis. Internal audit's reports should identify owner, accountabilities, and timescales for each management action; • any thematic issues identified across the organisation; • an independent view of management's reporting on the risk management of the organisation, including a view on management's remediation plans, highlighting significant delays; and • a review of any post-mortem and 'lessons learned' analysis if a significant adverse event has occurred at an organisation. • at least annually, internal audit should provide the audit committee with an assessment of the overall effectiveness of the governance, and risk and control framework of the organisation, and its conclusions on whether the organisation's risk appetite is being adhered to, together with an analysis of themes and trends emerging from internal audit work and their impact on the organisation's risk profile.

Interaction with risk management, compliance and finance	• Internal audit should include within its scope an assessment of the adequacy and effectiveness of the control functions (e.g. finance, HR, compliance, legal, health & safety and risk management). Any judgement which results in less intensive internal audit scrutiny should only be made after an appropriate evaluation of the effectiveness of that specific function in relation to the area under review. • The objectivity of internal audit is strongest if it is neither responsible for, nor part of, the "control" functions and such separation has to be preferred.
Independence and authority of internal audit	• The chief internal auditor should be at a senior enough level within the organisation to give him or her the appropriate standing, access and authority to challenge the executive. • Internal audit should have the right to attend and observe all or part of executive committee meetings and any other key management decision-making fora. • Intenal audit should have sufficient and timely access to key management information and a right of access to all of the organisation's records necessary to discharge its responsibilities. • In organisations in which the internal audit function is outsourced this Code still applies, and the chief internal auditor should always be employed directly by the organisation to ensure they have sufficient and timely access to key management information and decisions. • The audit committee should be responsible for appointing the chief internal auditor and removing him/her from post. The primary reporting line for the chief internal auditor should be to the chair of the audit committee and if there is to be a secondary executive reporting line, this should be to someone who promotes, supports and protects internal audit's independent and objective voice. Ordinarily this should be the CEO but, with the agreement of the chair of the audit committee, it could be to another member of executive management. • Where the tenure of the chief internal auditor exceeds seven years, the audit committee should discuss, on an annual basis, the chair's assessment of the chief internal auditor's independence and objectivity.
Resources	• The chief internal auditor should ensure that the audit team has the skills and experience, including technical subject matter expertise, commensurate with the scale of operations and risks of the organisation. • The audit committee should be responsible for approving the internal audit budget and, as part of the board's overall governance responsibility, should disclose in the annual report whether it is satisfied that internal audit has the appropriate resources.
Quality Assurance	• The board or the audit committee is responsible for evaluating the performance of the internal audit function on a regular basis. In doing so it will need to identify appropriate criteria for defining the success of internal audit. Delivery of the audit plan should not be the sole criterion in this evaluation. • Internal audit functions of sufficient size should develop a quality assurance and improvement programme to comment on internal audit's understanding and identification of risk and control issues and adherence to audit methodology and procedures. The results of these assessments should be reported to the audit committee at least annually. • Irrespective of the size of the organisation, the audit committee should obtain an independent and objective external quality assessment of the internal audit function at appropriate intervals, and as a minimum be subject to review at least every five years.

For further information:

The Code of Practice is available at:
www.iia.org.uk/internal-audit-code-of-practice.

Deloitte view

- We are supportive of the development of this Code of Practice and believe that the Code produces a useful and challenging framework.
- The recommendations will be stretching for some companies, but it is for audit committees to use this Code as a benchmark to review their internal audit function and to explain why they believe current arrangements remain appropriate.
- Companies wishing to follow the Code of Practice will need to consider the resourcing and skills implications to meet the broad range of activities suggested particularly if:
  - internal audit is to comment on whether information used in decision making is fair, balanced and reasonable; and,
  - there is an expectation internal audit will provide an annual assessment of the organisation's governance, risk and control framework and whether its risk appetite is being adhered to.

The Deloitte Academy

The Deloitte Academy provides support and guidance to boards, committees and individual directors, principally of the FTSE 350, through briefings on relevant board topics. The Deloitte Academy is available to board directors of listed companies, and includes access to the Deloitte Academy business centre in Deloitte's offices at 1 New Street Square, between Covent Garden and the City.

Members receive copies of our regular publications on Corporate Governance and a newsletter. A dedicated members' website www.deloitteacademy.co.uk is made available so members can register for briefings and access additional relevant resources.

For further details about the Deloitte Academy please email enquiries@deloitteacademy.co.uk

Contacts – Centre for Corporate Governance

Tracy Gordon 020 7007 3812 or trgordon@deloitte.co.uk
Corinne Sheriff 020 7007 8368 or csheriff@deloitte.co.uk
William Touche 020 7007 3352 or wtouche@deloitte.co.uk

Contacts – Global Internal Audit Lead

Peter Astley 020 7303 5264 or pastley@deloitte.co.uk

Deloitte.

Designed by CoRe Creative Services. RITM0387481