Deloitte.

The Deloitte Academy
July 2019

Governance in brief

IIA consultation raises the bar for 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 through the development of an Internal Audit Code of Practice.
- This builds on earlier work developing a similar Code of Practice for financial services firms.
- The draft Code aims to be regarded as a benchmark of good practice against which organisations can assess their internal audit function.
- This is a far reaching Code and will raise the bar for many organisations, both public and private, should they wish to comply with the Code. The following recommendations are particulary far reaching, recommending that internal audit:
  - 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;
  - 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.
- Companies are encouraged to respond to the consultation as there will be challenges associated with implementation.

The draft Code of Practice

The recommendations contained within the Code are principles-based, rather than establishing detailed rules. They are written in the context of a reasonably sized organisation operating within the UK and Ireland. Smaller organisations and branches of non-UK headquartered organisations in particular might need to make some modifications to the detail, in light of their size, risk profile and internal organisation and the nature, scope and complexity of their operations.

The consultation is seeking views on the draft Internal Audit Code of Practice which 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. • 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 of internal audit	• Internal audit's scope should be unrestricted – its scope should include information presented to the board and its committees. • 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 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. • 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.

Priorities of internal audit	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 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 if these events (business process change, new products and services, outsourcing decisions and acquisitions/divestments etc) are sufficiently high risk to warrant involvement on a real time basis. Internal audit should evaluate whether the information used in such key decision-making is fair, balanced and reasonable. • 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	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; • 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 'lesson 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.
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). • Internal audit should not rely exclusively on the work of the "control" functions and should itself assess the design and effectiveness of the controls operated by the function in question, and form its own view of the risks to which the organisation is exposed.

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. • 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 the CEO. • 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. • 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 adherance to audit methodology and procedures. The results of these assessments should be reported annually to the audit committee. • Irrespective of the size of the organisation, the audit committee should obtain an independent external assessment of the internal audit function at least every five years.

Next steps

The IIA is asking the following questions:

1. Which companies, organisations and sectors should the new Internal Audit Code of Practice cover and what should its scope be?
2. How far should there be independence between the second and third lines of defence?
3. Should internal audit have the right to attend and observe Executive Committee meetings?
4. Should the new Code include guidance and best practice on the outsourcing of internal audit provision?
5. Should the secondary executive reporting line be to the CEO, or should we adopt a more flexible approach in the new Code?
6. Should the new Code include guidance on how an internal audit function may provide assurance services where it had previously performed consulting services?
7. Are there any other matters which should be addressed in the Internal Audit Code of Practice?

Responses to the consultation are requested by Friday 11th October.

For further information:

The full consultation paper is available at:
https://www.iia.org.uk/research-and-insight/internal-audit-code-of-practice-consultation/

Deloitte view

- We are supportive of the development of this Code of Practice and believe that the consultation draft 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 or to make changes identified.
- 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.
- In our opinion having a second reporting line to the CEO is helpful as this emphasises that internal audit is an "all business function". However, an expectation that internal audit attends executive committee meetings may be of limited value in practice and could compromise the objectivity of internal audit.

The Deloitte Academy

The Deloitte Academy provides support and guidance to boards, committees and individual directors, principally of the FTSE 350, through a series of briefings and bespoke training. Membership of the Deloitte Academy is free to board directors of listed companies, and includes access to the Deloitte Academy business centre between Covent Garden and the City.

Members receive copies of our regular publications on Corporate Governance and a newsletter. There is also a dedicated members' website www.deloitteacademy.co.uk which members can use to register for briefings and access additional relevant resources.

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.

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

Designed by CoRe Creative Services. RITM0303315