Chartered Institute of Internal Auditors

Consultation from the Chartered Institute of Internal Auditors for the

Internal Audit Code of Practice

Consultation on the draft code

Closing date: Friday 11 October 2019
Issued: Monday 15 July 2019

Contents

Foreword

The collapse of Carillion has led to a wide-ranging review of the UK's corporate governance framework, including the audit regime. This creates challenges for internal audit, but equally it provides an opportunity to enhance the role of the internal audit profession as a cornerstone of good corporate governance.

That is why we are now responding to this challenge by consulting with relevant stakeholders – both inside and outside of the profession - on the development of an Internal Audit Code of Practice. This new Code aims to embed best practice and raise the bar right across the profession.

The development of this new Code builds on the Chartered IIA's vital work in developing a similar Code of Practice for financial services firms which has been a great success in improving the scope, skills and status of internal audit. Our ambition is that the new Code will achieve the same for the profession in other sectors.

Following the financial crisis a common critique of internal audit within the financial services sector was that it was not taken seriously enough by senior stakeholders within organisations. However, it is notable that within two years of the Financial Services Code being introduced, 81% of Heads of Internal Audit had a secondary reporting line to the CEO (up from 63%), 84% attended the Executive Committee (up from 48%) and 37% had a rank equivalent to CFO (up from 19%).

The Financial Services Code was a success in part because it was principles based, whilst at the same time setting clear standards. So in the development of the new Code, we need to give careful consideration to how far we want the Internal Audit Code of Practice to stretch the performance of the internal audit profession, whilst at the same time because, it will be a voluntary code, ensuring that as many organisations as possible feel able to sign up to it.

Once agreed and published, the new Code will provide an industry benchmark for best practice internal audit. It will also provide a gauge by which boards, audit committees and where appropriate UK regulatory authorities can assess the role, function and effectiveness of internal audit functions.

We would be delighted to hear your views on the draft Code we have now published and invite you to respond to the consultation questions listed on pages 13 and 14 which cover the key issues we have identified that require further thought and consideration.

Brendan Nelson, Audit Committee Chair, BP and Chair, Internal Audit Code of Practice Steering Committee

General information

Consultation details and information on how to respond

The consultation is seeking views on the draft Internal Audit Code of Practice around a series of key questions covering some of the main issues associated with this new guidance for the internal audit profession.

Issued: Monday 15 July 2019

Respond by: Friday 11 October 2019

Responses can be emailed to: iiapolicy@iia.org.uk

When responding, please state whether you are responding as an individual or representing the views of an organisation. Please try to respond directly to the questions posed, although if you have further comments to make that are of relevance to the development of the new Code, you are welcome to provide them.

Audiences

Whilst we will consider views from all interested stakeholders, we particularly welcome views from internal audit professionals, executive and non-executive company directors (especially Audit Committee Chairs and members), other relevant professional membership bodies, professional services firms, relevant regulatory bodies, business membership groups, shareholder and investor groups, relevant research bodies and think tanks.

The Internal Audit Code of Practice Steering Committee

The development of the Internal Audit Code of Practice is being overseen by an independent Steering Committee that has been established by the Chartered IIA.

The members of the committee are as follows:

- Brendan Nelson, Audit Committee Chair, BP (Committee Chair)
- Byron Grote, Audit Committee Chair, Tesco and Anglo American
- David Lindsell, Audit Committee Chair, Drax Group
- Carolyn Clarke, Head of Audit, Risk and Control, Centrica
- Paul Kaczmar, Director of Internal Audit, Michael Page
- Angela O'Hara, Director Assurance & Risk, Johnson Matthey
- Colin Gray, Senior Vice President, Risk and Assurance, InterContinental Hotels Group
- Paul Boyle, Chairman, Protect (Committee Adviser)
- Paul George, Executive Director, Corporate Governance & Reporting, Financial Reporting Council (Committee Observer)
- Dr Ian Peters MBE, Chief Executive, Chartered IIA (Committee Observer)

The committee is also being supported by a secretariat provided by the following Chartered IIA staff:

- Gavin Hayes, Head of Policy and External Affairs, Chartered IIA
- Liz Sandwith, Chief Professional Practice Advisor, Chartered IIA

Draft Internal Audit Code of Practice

Context

The recommendations which follow are aimed at enhancing the overall effectiveness of internal audit, and its impact, within organisations operating in the UK and Ireland. They can be regarded as a benchmark of good practice against which organisations can assess their internal audit function. The intended audience for the Internal Audit Code of Practice includes chief internal auditors, executive and non-executive directors, and in particular members of audit and risk committees, and where appropriate regulatory bodies.

The Code should be applied in conjunction with the existing International Professional Practices Framework (IPPF) published by the Global Institute of Internal Auditors, which includes the International Standards for the Professional Practice of Internal Auditing ('the IIA Standards'). The code builds on those IIA Standards; and seeks to increase the effectiveness and impact of internal audit within organisations by clarifying expectations and requirements.

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 in all private sector organisations 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: but all should comply with the principles.

[A] Role and mandate of internal audit

1. 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.

   It does this by assessing whether all significant risks are identified and appropriately reported by management to the board and executive management; assessing whether they are adequately controlled; and by challenging executive management to improve the effectiveness of governance, risk management and internal controls. The role of internal audit should be articulated in an internal audit charter, which should be publicly available.

2. 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.

[B] Scope and priorities of internal audit

3. Internal audit's scope should be unrestricted.

   There should be no aspect of the organisation which internal audit should be restricted from looking at as it delivers on its mandate. Whilst it is not the role of internal audit to second guess the decisions made by the board and its committees, its scope should include information presented to the board and its committees as discussed further below.

4. Risk assessments and prioritisation of internal audit work.

   In setting its scope, internal audit should form its own judgement on how best to segment the audit universe given the structure and risk profile of the organisation. It 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. Internal audit's independent view should be informed, but not determined, by the views of management. In setting out its priorities and deciding where to carry out more detailed work, internal audit should focus on the areas where it considers risks to be higher.

   Internal audit should make a risk-based decision as to which areas within its scope should be included in the audit plan – it does not necessarily have to cover all of the scope areas every year. Its judgement on which areas should be covered in the audit plan, and on the frequency and method of audit cycle coverage, should be subject to approval by the audit committee.

5. Internal audit coverage and planning.

   Internal audit plans, and material changes to internal audit plans, should be approved by the audit committee. They should have the flexibility to deal with unplanned events to allow internal audit to prioritise emerging risks. Changes to the audit plan should be considered in light of internal audit's ongoing assessment of risk.

6. Scope of internal audit.

   The scope of internal audit's work should be regularly reviewed to take account of new and emerging risks. Where relevant, internal audit should assess not only the process followed by the organisation's first and second lines of defence, but also the quality of their work.

As a minimum, internal audit should include within its scope the following areas:

a. Internal governance.

   Internal audit should include within its scope the design and operating effectiveness of the internal governance structures and processes of the organisation.

b. The information presented to the board and executive management for strategic and operational decision-making.

   Internal audit should include within its scope the processes and controls supporting strategic and operational decision-making. It should assess 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.

c. The setting of, and adherence to, the risks the entity is willing to accept (risk appetite).

   Internal audit is not responsible for setting the risk appetite but should assess whether the risk appetite has been established and reviewed through the active involvement of the board and executive management. It should assess whether risk appetite is embedded within the activities, limits and reporting of the organisation; and it should report annually to the audit committee its conclusions on whether the organisation's risk appetite is being adhered to.

d. The risk and control culture of the organisation.

   Internal audit should include within its scope the risk and control culture of the organisation. This should include assessing whether the processes (e.g. appraisal and remuneration), 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.

   Internal audit should consider the attitude and assess the approach taken by all levels of management to risk management and internal control. This should include management's actions in addressing known control deficiencies as well as management's regular assessment of controls.

e. Key corporate events.

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

f. Outcomes of processes.

Internal audit should evaluate the design and operating effectiveness of the organisation's policies and processes. In doing so, it should not adopt a 'tick box' approach based purely on the design of processes and should always consider the actual outcomes which result from their application, assessed against the espoused values, ethics, risk appetite and policies of the organisation.

[C] Reporting results

7. Internal audit should be present at, and issue reports to the appropriate governing bodies, including the board audit committee, and any other board committees as appropriate. The nature of the reports will depend on the remits of the respective governing bodies.

8. Internal audit's reporting to the board 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 owners, 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 (which might include restricting further business until improvements have been implemented) highlighting areas where there are significant delays;
- a review of any post-mortem and 'lesson learned' analysis if a significant adverse event has occurred at an organisation. Any such review should assess both the role of the first and second lines of defence and internal audit's own role; and
- at least annually, 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.

[D] Interaction with risk management, compliance and finance

9. In most organisations there will be some functions (e.g. finance, HR, compliance, legal, health & safety and risk management) whose responsibilities include designing and/or operating controls over risks which arise in other parts of the organisation. In some cases these functions (hereafter referred to as "control functions") will also have direct responsibility for managing certain business risks (e.g. a finance function will typically design and operate controls over expenditure incurred in other parts of the organisation but will also have direct responsibility for managing treasury and tax risks). Functions with such control responsibilities have substantial potential to contribute to the effectiveness of governance, risk management and internal controls in an organisation. However, the existence, scope and effectiveness of these functions will in practice vary considerably.

10. Internal audit should include within its scope an assessment of the adequacy and effectiveness of the control functions. This assessment should involve informed judgement as to what extent it is appropriate to take account of relevant work undertaken by others, such as risk management, compliance or finance in either its risk assessment or in the determination of the level of audit testing required for the activities under review. 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. 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.

11. The objectivity of internal audit is strongest if it is neither responsible for, nor part of, the "control" functions and such separation is to be preferred. However, the purpose and skills of internal audit is complementary to that of the "control" functions and, in some cases, organisations may assign responsibility for some "control" functions to the Chief Internal Auditor. A common example is for a joint head of Risk and Internal Audit.

12. In cases where the Chief Internal Auditor has been assigned some other "control" functions the Audit Committee should ensure that the additional responsibilities of the Chief Internal Auditor:

    a. do not undermine his/her ability to give appropriate attention to their internal audit responsibilities

    b. do not impair his/her independence from management

    c. are appropriately documented in the internal audit charter.

13. The board should also recognise that the Chief Internal Auditor is not able to make an objective assessment of the effectiveness of the additional functions for which he/she has responsibility and that it may be desirable to commission an external assessment of those functions.

[E] Independence and authority of internal audit

14. 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. Subsidiary, branch and divisional heads of internal audit should also be of a seniority comparable to the senior management whose activities they are responsible for auditing.

15. 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.

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

    In organisations in which the internal audit function is outsourced, the chair of the audit committee should identify an appropriate individual responsible for ensuring that the chief internal auditor has sufficient and timely access to key management information and decisions.

17. The primary reporting line for the chief internal auditor should be to the chair of the audit committee. In exceptional circumstances, the board may wish for internal audit to report directly to the chair of the board, or delegate responsibility for the reporting line to the chair of another

board committee, provided the chair and all the other committee members are independent non-executive directors. The reporting line must avoid any impairment to internal audit's independence and objectivity.

18. The audit committee should be responsible for appointing the chief internal auditor and removing him/her from post.

19. The chair of the audit committee should be accountable for setting the objectives of the chief internal auditor and appraising his/her performance at least annually. It would be expected that the objectives and appraisal would take into account the views of the chief executive. This appraisal should consider the independence, objectivity and tenure of the chief internal auditor. Where the tenure of the chief internal auditor exceeds seven years, the audit committee should explicitly discuss annually the chair's assessment of the chief internal auditor's independence and objectivity**.**

20. The chair of the audit committee should be responsible for recommending the remuneration of the chief internal auditor to the remuneration committee. The remuneration of the chief internal auditor and internal audit staff should be structured in a manner such that it avoids conflicts of interest, does not impair their independence and objectivity and should not be directly or exclusively linked to the short-term performance of the organisation.

21. Subsidiary, branch and divisional heads of internal audit should report primarily to the group chief internal auditor, while recognising local legislation or regulation as appropriate. This includes the responsibility for setting budgets and remuneration, conducting appraisals and reviewing the audit plan. The group chief internal auditor should consider the independence, objectivity and tenure of the subsidiary, branch or divisional Heads of internal audit when performing their appraisals.

22. If internal audit has a secondary executive reporting line, this should be to the CEO in order to preserve independence from any particular business area or function and to establish the standing of internal audit alongside the executive committee members.

[F] Resources

23. 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. This may entail training, recruitment, secondment from other parts of the organisation or co-sourcing with external third parties.

24. The chief internal auditor should provide the audit committee with a regular assessment of the skills required to conduct the work needed, and whether the internal audit budget is sufficient to recruit and retain staff or procure other resources with the expertise, experience and objectivity necessary to provide effective challenge throughout the organisation and to the executive.

25. 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.

[G] Quality Assurance and Improvement Programme (QAIP)

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

27. Internal audit should maintain an up-to-date set of policies and procedures, and performance and effectiveness measures for the internal audit function. Internal audit should continuously improve these in light of industry developments.

28. Internal audit functions of sufficient size should develop a quality assurance and improvement programme, with the work performed by individuals who are independent of the delivery of the audit. The individuals performing the assessments should have the standing and experience to meaningfully challenge internal audit performance and to ensure that internal audit judgements and opinions are adequately evidenced.

    The scope of the QAIP review should include internal audit's understanding and identification of risk and control issues, in addition to the adherence to audit methodology and procedures. This may require the use of resource from external parties. The quality assurance work should be risk-based to cover the higher risks of the organisation and of the audit process. The results of these assessments should be presented directly to the audit committee at least annually.

29. Where the internal audit function is outsourced to an external provider, internal audit's work should be subject to the same QAIP work as the in-house functions. The results of this QAIP work should be presented to the audit committee at least annually for review. Heads of internal audit should report regularly to the audit committee on the actions or progress implementing the outcomes of the review.

30. In addition, the audit committee should obtain an independent and objective external assessment at appropriate intervals, irrespective of the size of the organisation. This could take the form of periodic reviews of elements of the function, or a single review of the overall function. In any event, the internal audit function as a whole should as a minimum be subject to a review at least every five years, as set out in the International Professional Practices Framework for internal audit. The conformity of internal audit with this guidance should be explicitly included in this evaluation. The chair of the audit committee should oversee and approve the appointment process for the independent assessor.

Consultation questions

1. Which companies, organisations and sectors should the new Internal Audit Code of Practice cover and what should its scope be?

Internal Audit has the potential to contribute to effective risk management and governance in both private and premium listed companies, as well as of course third sector organisations including major charities. We will therefore need to consider carefully which types of organisations the new Internal Audit Code of Practice should apply to.

We will need to consider whether the new Code should be primarily focused on publicly listed companies, or should private companies with an internal audit function also be in scope – particularly large private companies? Going even further than that, should the new Code be extended to third sector organisations? In due course, a Code could also be developed for the public sector.

2. How far should there be independence between the second and third lines of defence?

Does the draft Code adequately reflect the range of practices that organisations have adopted with regard to the existence or not of separate risk and compliance functions? And what does the Code need to say specifically about circumstances where risk and internal audit are combined?

3. Should internal audit have the right to attend and observe Executive Committee meetings?

Do you agree that we should now raise the bar for the profession and insist that internal audit have a seat at the table at the Executive Committee?

4. Should the new Code include guidance and best practice on the outsourcing of internal audit provision?

Is it desirable to develop further guidelines around outsourcing best practice? If so, what should these be?

5. Should the secondary executive reporting line be to the CEO, or should we adopt a more flexible approach in the new Code?

In the majority of organisations spanning all sectors there is a formal reporting line to the Audit Committee via the Audit Committee Chair.

However, whilst a secondary reporting line to the CEO is now common practice in the financial services sector, for other organisations it is often the case that they will have a secondary reporting line to another member of the executive management team such as the CFO.

In promoting internal audit best practice and in raising the bar across the profession, should we provide clear guidance that the secondary reporting line should be to the CEO? Or should we adopt a more flexible approach? If we adopt a more flexible approach, how do we mitigate the risk of potential conflicts of interest that could arise from a secondary reporting line (e.g. to the CFO)? As an alternative to a secondary reporting line to the CEO, would it be acceptable to have a secondary reporting line to another member of the executive management team?

6. Should the new Code include guidance on how an internal audit function may provide assurance services where it had previously performed consulting services?

The issue of safeguarding against compromise of objectivity where internal audit are asked to perform consultancy services is an important one to consider in the development of the new Internal Audit Code of Practice.

The current IIA Standards offer clear guidance in this respect. They state that the internal audit function may provide assurance services where it had previously performed consulting services, provided the nature of the consulting does not impair objectivity and provided objectivity is managed when assigning resources to the engagement, and that internal auditors may provide consulting services relating to operations for which they had previous responsibilities. If internal auditors have potential impairments to independence or objectivity relating to the proposed consulting services, the IIA Standards state that disclosure must be made to the engagement client prior to accepting the engagement.

In promoting best practice should the new Code also offer clear guidance on this issue?

7. Are there any other matters which should be addressed in the Internal Audit Code of Practice?

The questions we have asked cover some of the key issues and areas of importance we will need to consider carefully in the development of the Internal Audit Code of Practice. Inevitably there may be other areas of importance that we have not covered or thought about that we may need to address in order to make the Code a success. So, are there any other practical issues or ideas that you would like the Steering Committee to consider as part of this consultation?

About the Chartered Institute of Internal Auditors

The Chartered Institute of Internal Auditors (IIA) is the only professional body in the UK and Ireland solely dedicated to supporting, promoting and training internal auditors. We represent over 10,000 internal auditors working in private and public sector.

Our vision

Our vision is that professional internal audit will be recognised as essential to the success of organisations and their leaders; and that the Institute will be recognised as essential to the success of internal audit professionals.

Our mission

The Institute's mission is to support and develop internal audit professionals throughout their careers, and to promote the role and value of the profession. We aspire to be recognised as the authoritative professional body for the internal audit profession, and as widely influential amongst our stakeholders.

For any enquiries concerning this consultation please contact:

Gavin Hayes
Head of Policy & External Affairs

Chartered Institute of Internal Auditors,
13 Abbeville Mews,
88 Clapham Park Road,
London,
SW4 7BX

t. 020 7498 0101
e. iiapolicy@iia.org.uk
w. iia.org.uk