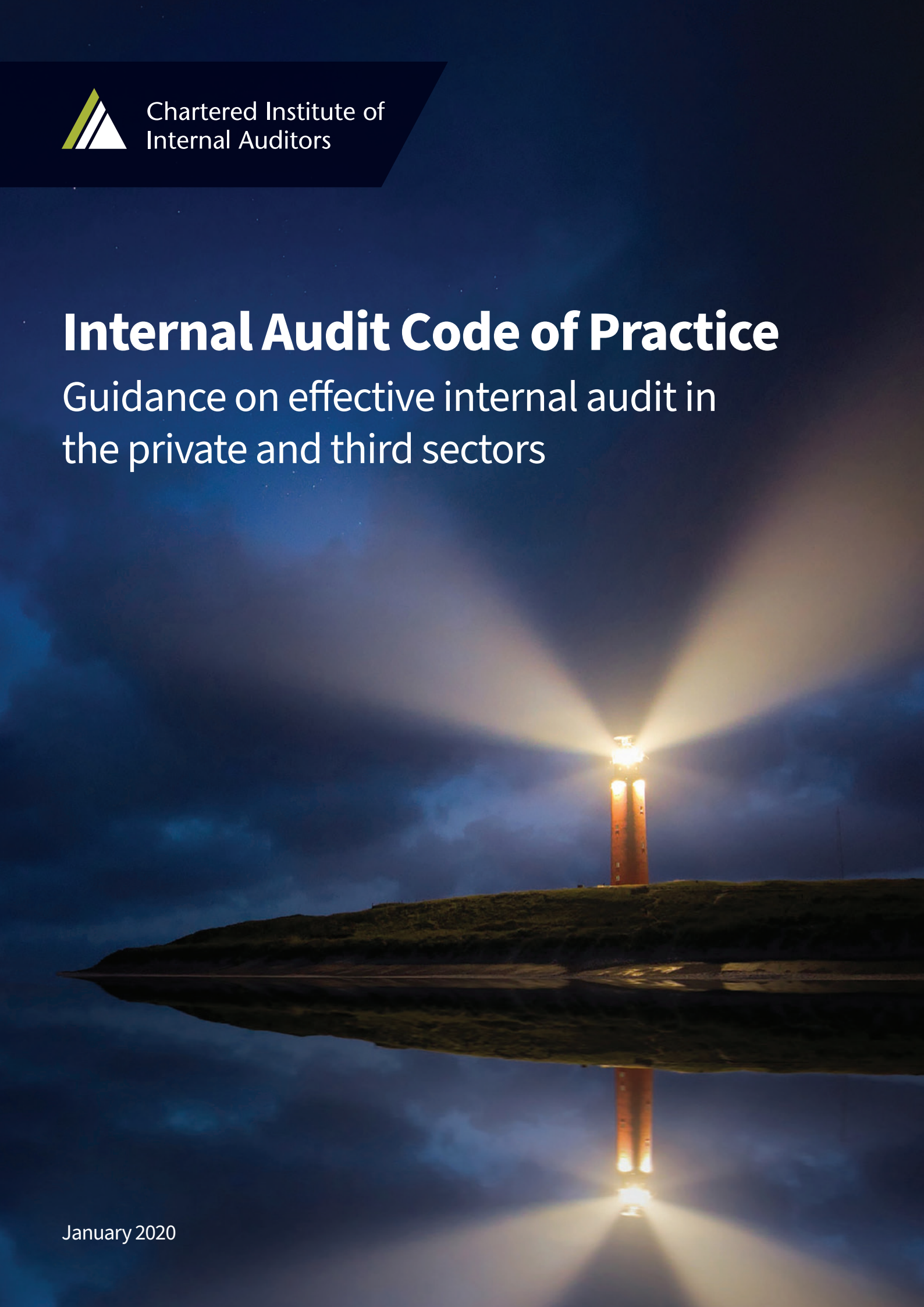
Chartered Institute of Internal Auditors

# Internal Audit Code of Practice

## Guidance on effective internal audit in the private and third sectors



January 2020

# **Foreword** from the Council

**We are pleased to publish our Internal Audit Code of Practice which provides guidance on effective internal audit in the private and third sectors. The Code is principles-based, and is intended as an industry benchmark, to help embed good practice internal audit and raise the bar across the profession.**

The guidance contained within the Code represents the final recommendations of the independent Internal Audit Code of Practice Steering Committee, which the Institute has accepted in full and now commends to the boards and internal audit professionals of all private and third sector organisations operating in the UK and Ireland.

The publication of this new Code further 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 Internal Audit Code of Practice delivers the same for the profession working outside of financial services in the private and third sectors.

The independent Steering Committee which oversaw the development of the Code was chaired by Brendan Nelson, the Audit Committee Chair of BP (and formerly of RBS), who was also involved in the development of our Financial Services Code and so the work really benefitted from that previous experience. Other committee members included audit committee chairs and chief internal auditors representing a diverse range of businesses from different sectors and sizes, along with the involvement of the Financial Reporting Council as an observer.

The final recommendations contained within the Code were made following a thorough twelve-week public consultation process in which the independent committee engaged and gathered the views of a range of stakeholders including internal audit professionals, executive and non-executive directors, professional bodies, business groups and the professional services firms.

The exercise resulted in a high level of engagement and debate on how to enhance internal audit's role as a cornerstone of good corporate governance, with seventy written responses received by the committee to the consultation.

The publication of this new guidance is both important and timely, given recent high-profile corporate collapses linked to governance deficiencies, most notably Carillion in January 2018, which has led to a wide-ranging review of the audit and corporate governance framework. This creates an opportunity to enhance internal audit's role in supporting non-executive and executive management, in organisations across the private and third sectors, to manage and mitigate their risks more effectively.

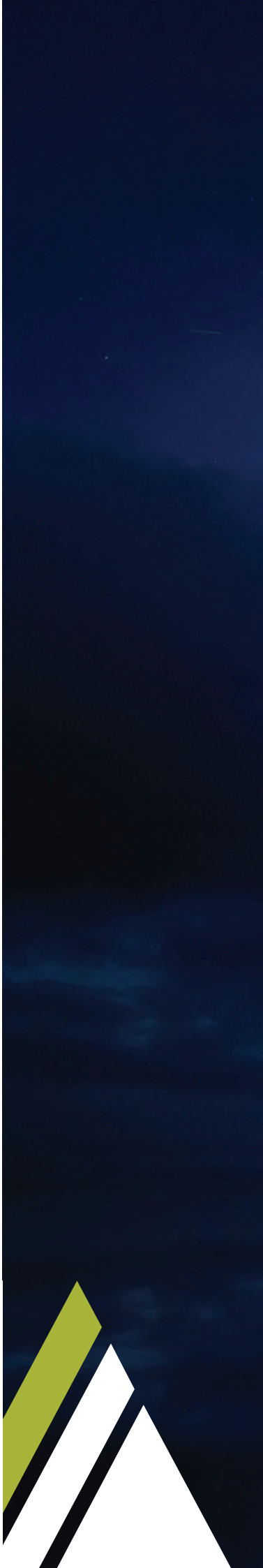
We therefore urge boards, and in particular audit committees, to embrace the key principles contained within the Code, so as to enhance the effectiveness of their internal audit functions. This will help internal audit to maximise its value and deliver its true potential.

Finally, we would like to express our sincere thanks to the members of the committee for their commitment, tenacity and diligence in developing the Code. We have no doubt that their exceptional work will deliver a more influential and effective internal audit profession, as well as contribute to better corporate governance in the UK and Ireland.

**The Council**

# Contents





# **Message** from the Chair

**The publication of the Internal Audit Code of Practice represents the final and unanimous recommendations of the independent Steering Committee established by the Chartered Institute of Internal Auditors. The aim of the guidance is to increase the effectiveness of internal audit functions in the private and third sectors.**

Building on the success of the Chartered IIA's Guidance on Effective Internal Audit in the Financial Services Sector ("Financial Services Code") we hope that this new Code has a similar impact at raising the scope, skills and status of the internal audit profession across a broader range of private and third sector organisations. In turn it should help to promote and strengthen good corporate governance.

The final Code has been issued following a full and comprehensive public consultation exercise which attracted a strong response from stakeholders, including seventy written responses submitted to the draft version of the Code that we published in July 2019. Indeed, the committee was impressed by the level of thought and consideration that went into the responses, and the overall support for the Code further validated the process. The committee has now considered carefully the results of the consultation, listened to the views of stakeholders, and made a number of changes as a consequence of that feedback.

One of the key themes from the written responses and in the one to one meetings we conducted with stakeholders, was the need for the Code to be modified to make it clearer that it should be applied proportionately, dependent on the size and complexity of the organisation. In response we have put greater emphasis on this and made it clearer in the introduction section of the Code.

For the Code now to be implemented successfully and for its recommendations to be effective, it is critical that it is actively supported by all relevant stakeholders. In particular this will require chief internal auditors, audit committee chairs (and members), boards and executive management working collaboratively in partnership to ensure the principles and recommendations contained within the Code are applied appropriately. I urge them to do just that.

Finally, I would like to offer my thanks to the members and observers of the independent Steering Committee for all their excellent work.

**Brendan Nelson,**
Chair, Internal Audit Code of Practice Steering Committee

# The Guidance

## Introduction

### *The purpose of the Code*

1. 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.

### *Who is it for?*

2. The intended audience for the 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.

3. 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. It is based on Effective Internal Audit in the Financial Services Sector ('Financial Services Code'), but internal audit functions in financial services should continue to follow the 'Financial Services Code' which contains provisions which are specific to financial services. Whilst it may prove useful for internal audit in the public sector, it is not drafted with the public sector specifically in mind and public sector internal audit functions should continue to follow the Public Sector Internal Audit Standards.

### *How should it be applied?*

4. The Code of Practice 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 Standards; and seeks to increase the effectiveness and impact of internal audit within organisations by clarifying expectations and requirements.

5. The Code is principles-based. It is expected that the procedural requirements of the Code should be applied proportionately, and therefore smaller organisations should apply the principles on which the Code is based and its procedural requirements in light of their size, risk profile and internal organisation and the nature, scope and complexity of their operations.

## A. Role and mandate of internal audit

6. 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.

7. 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

8. 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.

9. 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.

10. 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.

11. 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 viability of 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 on a timely basis if these events are sufficiently high risk to warrant involvement. 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

12. Internal audit should be present at, and issue reports to the relevant 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.

13. Internal audit's reporting to the board audit and 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 'lessons 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

14. 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. Functions with such control responsibilities have substantial potential to contribute to the effectiveness of governance, risk management and internal controls in an organisation.

15. 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.

16. 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.

17. 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.

18. 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

19. 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.

20. 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. This enables internal audit to understand better the strategy of the business, key business issues and decisions, and to adjust internal audit priorities where appropriate. It also facilitates a better working relationship with executive committee members.

21. 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 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.

22. The primary reporting line for the chief internal auditor should be to the chair of the audit committee.

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

24. 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.

25. 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.

26. 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.

27. If internal audit has a secondary 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 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. However, with the agreement of the chair of the audit committee the secondary reporting line could be to another member of executive management.

## F. Resources

28. 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.

29. 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.

30. 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)

31. 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.

32. 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.

33. 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.

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

35. In addition, the audit committee should obtain an independent and objective external quality 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 (IPPF) 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.

36. The external quality assessment should consider and report on compliance with this Code as well as with the International Professional Practices Framework (IPPF) and the International Standards for the Professional Practice of Internal Auditing ('the IIA Standards').

## H. Relationship with Regulators

37. The chief internal auditor should consider the impact of the regulatory environment and have an open, constructive and cooperative relationship with relevant regulators.

## I. Relationship with External Audit

38. The chief internal auditor and the partner responsible for external audit should ensure appropriate and regular communication and sharing of information.

# The independent Steering Committee

**Brendan Nelson**
Audit Committee Chair, BP
(Committee Chair)

**Byron Grote**
Audit Committee Chair,
Tesco and
Anglo American

**David Lindsell**
Audit Committee Chair,
Drax Group and
Cancer Research UK

**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

## Observers to the Committee

**Paul Boyle**, Chairman,
Protect (Committee Adviser)

**Paul George**, Executive Director,
Corporate Governance & Reporting,
Financial Reporting Council

**Dr Ian Peters MBE**, Chief Executive,
Chartered IIA

## Support to the Committee

**Gavin Hayes**, Head of Policy and External Affairs,
Chartered IIA

**Liz Sandwith**, Chief Professional Practices
Adviser, Chartered IIA

# About the Chartered Institute of Internal Auditors

**The Chartered Institute of Internal Auditors is the only professional body dedicated exclusively to training, supporting and representing internal auditors in the UK and Ireland.**

We have 10,000 members in all sectors of the economy.

First established in 1948, we obtained our Royal Charter in 2010. Over 2,000 members are Chartered Internal Auditors and have earned the designation CMIIA. About 1,000 of our members hold the position of head of internal audit and the majority of FTSE 100 companies are represented among our membership.

Members are part of a global network of 200,000 members in 170 countries, all working to the same International Standards and Code of Ethics.

Chartered Institute of
Internal Auditors

13 Abbeville Mews
88 Clapham Park Road
London SW4 7BX

tel 020 7498 0101
email info@iia.org.uk

**Further guidance on this Code and frequently asked questions will be made available on the Institute's website.**

Chartered Institute of
Internal Auditors