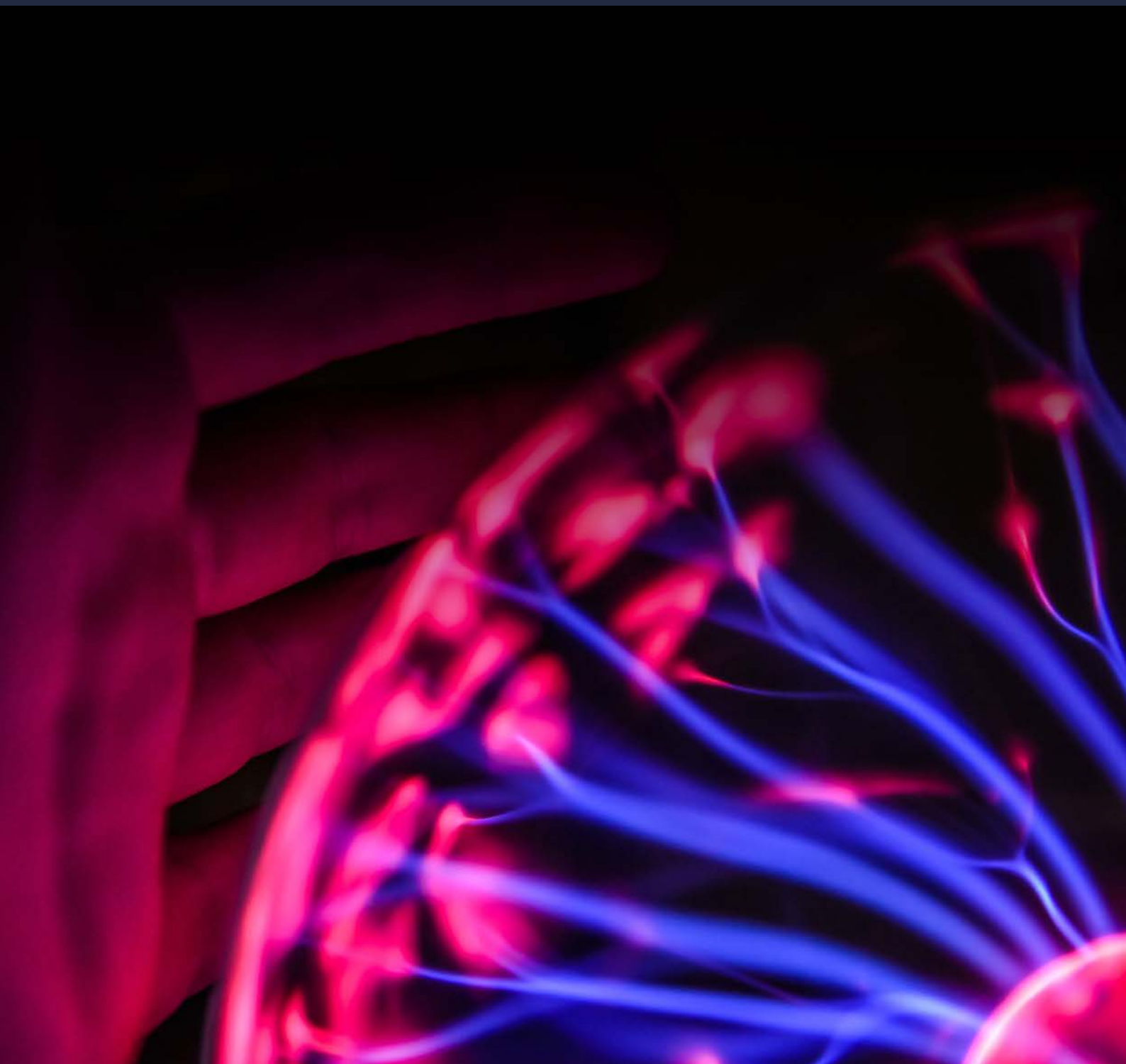
Chartered Institute of Internal Auditors

IoD *Inspiring* **business**

Harnessing the power of internal audit

A good corporate governance guide for audit committees and directors



Introduction

Internal audit is potentially one of the most powerful tools in the audit committee's armoury. This guide is designed to help the audit committee and other stakeholders to harness that power for the good of their organisations.

When properly resourced, positioned and targeted, professional internal audit provides the kind of insight that boards need to make effective decisions. Internal audit can provide independent assurance over how well the business is managing its risks, taking advantage of fast-moving opportunities and whether its corporate governance processes are operating effectively. Internal auditors who follow the International Professional Practices Framework (IPPF) not only bring technical rigour to their assurance activities, they continually improve the quality of their work through formal internal and external assessments – a process that helps improve the overall corporate governance of the organisation.

Getting governance right is particularly important today in light of both the rapid digitalisation of the business world and recent high-profile corporate failures. The potential for the rapid demise of well-known businesses is a reality that boards need to face. The retailer BHS and the facilities management and construction company Carillion, for instance, both seemed to be stable businesses with strong track records. But while there will be unique circumstances in every failure, the post mortems of such events usually reveal serious failings in corporate governance and culture.

The risk of failure in such areas should be mitigated by enhancing the role of internal audit. Over the past decade or so, internal audit has been moving out of the back office in many organisations to play a leading role in helping businesses get to grips with today's dynamic risk landscape. Heads of internal audit (HIAs) have become boards' trusted advisors on an increasingly complex range of risks. Cutting-edge internal audit can help businesses deal with a wide variety of issues outside of the compliance arena – from data privacy and automation, to political uncertainty and reputation risk.

The revised UK Corporate Governance Code, which came into effect in January 2019 (see *Appendix One*), places the difficult issues of workplace and organisational culture firmly on the board's agenda – another key area for internal audit. The Wates Corporate Governance Principles for Large Private Companies say that those companies must report on how they are implementing and managing internal controls, which is an intrinsic element of good corporate governance – bringing them more in line with publicly-listed businesses. Those enterprises may need or find they are likely to benefit from internal audit.

"Cutting-edge internal audit can help businesses deal with a wide variety of issues outside of the compliance arena – from data privacy and automation, to political uncertainty and reputation risk."

Internal audit can also play an important role in ensuring projects run on time, new initiatives get off the ground and that environmental and social impacts are in line with organisations' – and society's – aspirations. To help audit committees harness that power, this guide poses eight key questions. Because organisations differ greatly, there are few right or wrong answers. Yet working through the issues raised by this guide should enable stakeholders to understand where they need to focus their corporate governance and internal audit improvement efforts. In doing so, they will find themselves better prepared for the challenges ahead.

Harnessing the power of internal audit – key questions

1. What is internal audit's role and mandate?

Internal audit's role is to help the board and executive management protect and enhance the assets, reputation and sustainability of the organisation. Internal audit adds most value when it has the authority to cover the full portfolio of risks that the organisation faces – for instance, cultural, strategic, operational, reporting and compliance – to provide formal assurance audits and advisory activities as and when required. Many audit committee chairs consider their head of audit to be a trusted advisor – someone who can act as a sounding board for the committee and speak with authority and objectivity about the entire business and the risks it faces.

To operate effectively, internal audit's role should be mandated in a formal internal audit charter. The charter gives the audit function the audit committee's formal backing to operate anywhere in the business. It will be tailored to the organisation's unique structure, range of activities, market sector, geographical locations and strategic and operational risks. Reviewing the charter on a regular basis helps the audit committee and internal audit to stay tuned in to the changes and emerging risks impacting the business.

2. What is internal audit's scope?

In recent years the scope of internal audit has widened massively to mirror the risks and opportunities that a dynamic and rapidly digitalising world presents. The days when internal audit focused solely on controls over financial reporting are gone. The revised UK Corporate Governance Code continues this trend by widening audit's scope further to pay explicit attention to culture risk, for instance.

The audit committee should see the scope of internal audit's role as unrestricted. That does not mean unstructured. In consultation with their audit committees, HIAs generally develop a risk-based, strategic audit plan (normally spanning three to five years) and an annual audit plan with contingency built in to manage emerging risk areas and unexpected events.

While each business will face specific challenges, according to the Chartered IIA's recent paper *Risk in Focus 2019* internal auditors have been focusing increasingly on emerging risks including:

WORKPLACE CULTURE

Trends in the world of social media can have a rapid and lasting impact in the workplace. Examples of sexual harassment have spread into the business world since the #MeToo movement exploded last year. Given the impact of such campaigns, it is clear that corporate values will increasingly need to reflect those trending in society.

The revised UK Corporate Governance Code puts staff diversity and corporate culture firmly on the agenda. The updated Code includes new principles and provisions on diversity and inclusion, as well as on the alignment of company purpose, strategy and values with corporate culture. The Code highlights a continuous role for the board in establishing, promoting, assessing and monitoring the desired corporate culture.

The Chartered IIA has done a lot of thought leadership in this area – including its report *Organisational Culture – Evolving approaches to embedding and assurance.*

For example, boards need assurance that a culture of learning from mistakes, rewarding the right behaviour, and systems and processes that produce the desired behaviours are being embedded across their organisations. A statement of values is not sufficient on its own: boards need to know that 'espoused' values are the same as actual values on the ground. Providing assurance to boards around values on the ground, however, is just part of the picture as culture is not merely the articulation of an organisation's values.

Internal auditors should be seen as a key resource. Many have begun to address these issues by looking at soft controls within their organisations, such as how senior management assure that corporate values are reflected in everyday behaviour and whether excessive risk-taking is incentivised. Many are finding ways to provide assurance that potentially toxic cultures are not harming people in the workplace.

COMMUNICATIONS RISK AND REPUTATION

Building a corporate reputation can take years – destroying it a matter of days. High-profile customer communications failures are frequently reported in the media. The ramifications for those businesses on reputation, share price and profitability can be painfully public and long lasting.

Any number of incidents can damage reputation, from customer data leaks and ill-conceived marketing campaigns to shabby customer service. It is often the way in which an organisation responds to such events that can make or break its reputation, and internal audit can have a central role to play in safeguarding the enterprise.

Internal auditors are increasingly providing assurance around communications risk by ensuring management has established clear roles, responsibilities, ownership and accountability for the messages it puts out. Robust sign-off processes, documented communications guidelines and policies all help to mitigate potential risk – as does making sure that posting on social media is treated as seriously as other forms of corporate communication.

DATA PRIVACY AND CYBERSECURITY

Most internal audit departments will have been involved in testing their organisation's preparations for the European Union's General Data Protection Regulation (GDPR), which came into force in May 2018. Not only are data privacy laws changing globally – for example the California Consumer Privacy Act of 2018, which mirrors many of the provisions of GDPR – the effective management and use of data has become an issue of competitive advantage.

If they have not already done so, there is scope for internal audit to assess the extent to which their organisation has established a data strategy and data governance standards. Audit can help businesses consider how data is managed, the extent to which it successfully drives value (revenues and profits) and supports the company's objectives and corporate strategy – not just in the business, but throughout the extended supply chain. This data strategy should be closely aligned with the organisation's cybersecurity strategy, as any loss of data to hackers or internal actors will result in a loss of value.

POLITICAL UNCERTAINTY

The recent rise of protectionist trade policies and the decision of the UK to leave the European Union pose significant risks to businesses. The US sanctions war with China, for example, has global ramifications and the uncertainty over trading terms that has emerged from the Brexit discussions ripple throughout Europe and beyond.

It is debatable whether trade protectionism and export sanctions, and geopolitics more generally, are specifically auditable risks. But the ability of organisations to respond in a timely and effective way to policy and legislative changes by putting into effect contingency and mitigation strategies is something internal audit can help with.

Additional risk assessments of entire supply chains can help to determine the potential for disruption, increased costs and depressed sales. Audit can provide assurance to management and the board that sufficient time and resources are being directed towards such efforts. It can provide insight on the process of evaluating strategic decisions and on tactics designed to react appropriately to political risks.

There is also value to be added in assuring that the organisation's compliance and procurement functions are on top of export controls and sanctions. The board may require assurance, for example, that compliance efforts are linked to strategic decision-making processes so that as the prohibition of trade in a sanctioned market increases, for instance, the business can weigh up its options for entering other geographic markets.

AUTOMATION AND DIGITALISATION

The cost and efficiency benefits of automation and other digital processes are well known – as are the potential downside risks of high-cost IT projects.

There are a range of ways internal audit can help organisations benefit from their investment in such areas. For example, internal audit can assess whether projects are aligned with the corporation's strategy in a way that is documented and specific. It can provide assurance that each project focuses on the exact processes that will be improved, can provide evidence on how they will be improved and include key performance indicators to measure the success of the new technology once it is operational – as well as ensuring management has created key risk indicators that can alert the business to potential failures. These issues have been covered extensively in the IIA's book, *Auditing and Disruptive Technologies*.

3. How should internal audit be resourced?

Audit committees can pose three questions when it comes to resources: does internal audit have the capacity to do the amount of work required of it? Does it have the capability to do the work well in terms of skills and knowledge? Is the audit team suitably qualified?

The first question can be answered by the HIA and the audit committee together by looking at the risk-based annual audit plan and the strategic audit plan and calculating the function's capacity to carry out those tasks. Because individual audits are linked to principal risks and the organisation's objectives and goals, these calculations can also reveal the potential impact of any resource limitations, such as on principal risks where there is a lack of assurance in relation to the effectiveness of controls to mitigate the risk. The audit committee has the final say on whether any principal risk areas will not be covered by internal audit through budgetary or resource constraints.

Naturally, the internal audit function should have the knowledge, skills, and competencies to execute the agreed plan. Technical skills are important, such as in IT or financial services regulation, but too little attention has been paid to developing soft skills and hiring people with good communication skills. Without effective interpersonal and communication skills auditors are unlikely to be able to clearly convey the value of their findings and recommendations and persuade management to take the appropriate actions.

It is part of the HIA's job to provide assurance to the audit committee that his or her team has the right mix of capabilities. If there are gaps, the audit committee should know what they are, how they could impact on the delivery of the strategic audit plan and how they are going to be addressed – for instance by the introduction of a guest auditor programme, or by co-sourcing or out-sourcing a particular area of work with an external provider, such as for cybersecurity assurance.

"Without effective interpersonal and communication skills auditors are unlikely to be able to clearly convey the value of their findings and recommendations and persuade management to take the appropriate actions."

Increasingly, internal audit functions are looking for internal auditors with qualifications – including the professional internal audit qualifications offered by the Chartered IIA. These not only ensure that audit staff are equipped with the right knowledge and professional skills, but that they have credibility in the eyes of other professionals within the business because they are operating according to global professional standards (the IPPF contains the global *IIA Standards*). This is particularly true for senior internal audit professionals such as HIAs. The Chartered IIA's training and professional qualifications cover every stage of an auditor's career development.

4. What is the relationship between the audit committee and internal audit?

The relationship between the audit committee and the HIA is of primary importance. For it to work well, the HIA and audit committee chair need to be able to speak openly to each other through both formal channels and informally. The HIA's line for formal communication to the audit committee needs to be a direct one if the function is to maintain its independence. But the HIA may want to give their 'gut feeling' about how things are, which may be difficult to express in a formal report or email.

In the digital age, internal auditors can make much greater use of both soft and hard indicators to reduce the subjectivity of their findings. Data from internal reporting systems can be aggregated and used to identify trends and to reveal issues of which the board may be unaware. The emergence of 'big data' provides scope for internal auditors to develop specific skills and work with data analysts to provide insight. This is a fast-developing area where audit committees and audit functions – together with other assurance providers – need to work closely and imaginatively together to develop experimental solutions to emerging problems.

Audit committee members and senior executives must be open to the idea that, at present, there may be less hard evidence in such areas compared to more traditional audits and accept the likelihood of grey areas where there may be differences of opinion. This may entail a change in culture and behaviour of the audit committee itself where audit findings are not crystal clear.

Having the right HIA in place is essential and audit committees should devote significant thought and effort to the process of appointing a professionally qualified HIA who follows the *IIA Standards*. Although the chief executive officer and the chief financial officer may play a role in the HIA hiring process, it is the audit committee's role to approve the functional profile and selection of the HIA. Equally, because of the HIA's independence and objectivity, audit committees should oversee the termination of the HIA's appointment and seek to understand the reasons behind any resignations.

> **"The relationship between the audit committee and the HIA is of primary importance. For it to work well, the HIA and audit committee chair need to be able to speak openly to each other through both formal channels and informally."**

5. Are all risks being managed?

Given the fast-changing nature of today's business world, managing the diverse range of traditional and emerging risks is a huge challenge. In an ideal world, front line managers would be aware of the risks their departments face and be capable of controlling those risks in real time (under the three lines of defence model outlined in Appendix Two). But because of the complexity of many types of risk, organisations also depend on a second line of defence to help managers comply with regulations, deal with enterprise-wide risk and emerging threats.

It is crucial that these different risk activities are adequately coordinated to avoid gaps and overlaps – a task that internal audit can perform because of its position as an independent oversight function within the corporate governance structure. Working with the head of risk and senior management, the HIA is able to develop an assurance map that can be shared with the audit committee. This can be helpful in making sure there is ownership of risk and clarity about responsibility when it comes to risk management.

But internal audit has a bigger role to play. Senior figures in the audit function should have an open and constructive relationship with the regulators for their industries. They should be able to share guidance and insights from the regulator with the business, to further inform the way that the organisation seeks to comply with rules and regulations.

Internal audit should also provide the audit committee with assurance on how well risk is governed across the entire enterprise, including how all lines of defence are operating. Done properly, this process can help the organisation develop a more robust risk culture in line with the aims of the revised UK Corporate Governance Code. The audit committee should support this culture of continuous improvement in risk governance by ensuring that this wider remit is both enshrined in the charter and that the task is given adequate resources.

6. How should internal audit's recommendations be monitored?

Normally, management will implement the agreed actions coming out of an internal audit or audit advisory project. The HIA will follow up to make sure those actions have been done effectively. In most cases, the HIA will have clearly communicated the value to management of acting on internal audit's recommendation and appropriate action will be taken to improve processes and controls.

When management fails to implement such actions within an agreed timeline, or where the measures have been ineffectively carried out, the HIA may bring the issue to the attention of the audit committee – especially when management is taking on an unacceptable level of risk.

The audit committee is likely to focus on how well – or otherwise – management have performed those actions, particularly in areas of major risk, and where measures have been outstanding for too long. When the audit committee feels that management is not implementing agreed actions, it should step in and invite the relevant directors and managers to a meeting to resolve outstanding issues. Where necessary, this should include inviting them to a meeting of the audit committee.

7. How should internal and external auditors work together?

Given the part played by some high-profile audit firms in recent corporate collapses, the audit committee should consider carefully any reliance it places on the assurance provided by external auditors on key areas such as financial controls.

> **“Internal audit should also provide the audit committee with assurance on how well risk is governed across the entire enterprise, including how all lines of defence are operating.”**

The role of external auditors is limited compared to that of internal audit. External auditors only provide assurance to shareholders, the board and senior management that the company’s financial statements provide a ‘true and fair’ view of its financial performance and current financial position. While this is an important statutory duty, external audit only looks at historical financial records during that process, so it is of limited use in assessing how well senior management is managing the organisation’s strategic, business and compliance risks. The role of internal audit, on the other hand, should be to provide assurance on the robustness of risk management across all areas.

Even so, it can be useful to include external audit’s planned work in the organisation’s assurance map. External auditors may wish to use internal audit’s findings in areas that touch on financial reporting: internal audit may benefit from any comments external audit provides in relation to internal control weaknesses noted in the course of the audit engagement. The audit committee needs to be satisfied that the relationship between the internal and external auditors does not become too interdependent or cosy.

8. How should the quality of internal audit's work be assessed?

Professional internal auditors follow the *IPPF*. It sets out best practice for internal auditors to develop and maintain a quality assurance and improvement programme that covers all aspects of the function. In addition, the Chartered IIA develops and provides many best practice guides, such as a code of practice for financial services companies, which are freely available to its members.

The audit committee can use the *IPPF* to see whether the audit programme has all the necessary components to provide insight on the efficiency and effectiveness of the internal audit function itself. The *IPPF* provides a great vehicle for the audit committee and the audit function to identify opportunities for continuous improvement.

The quality assurance and improvement programme includes both internal and external quality assessments, and a timetable listing key events so that the audit committee knows when and how the assessments will occur.

> **"The *IIA Standards* say an external quality assessment should be conducted at least once every five years and covers everything from audit methodology to the organisation's governance structure."**

Internal assessments include ongoing performance monitoring of internal audit by means of direct supervision as well as periodic self-assessments. Audit committees should ensure they receive the results and recommendations from these assessments in a timely manner, as they play a decisive role in helping to strengthen the effectiveness of the audit function and of the assessment process itself. The *IIA Standards* say an external quality assessment should be conducted at least once every five years and covers everything from audit methodology to the organisation's governance structure. While the HIA is likely to recommend an external assessor – either from the Chartered IIA or elsewhere – the audit committee should review the qualifications and independence of the external provider or review team and receive the report at the end of the assessment.

Those audit committees and internal audit functions that embrace the external quality assessment often see huge improvements in the performance of their audit functions. The Chartered IIA offers a very well-regarded external quality assurance and improvement programme.

Audit committees usually conduct their own assessment of internal audit annually. The questions posed in this document would be a useful way of starting that process.

APPENDIX ONE

Effective corporate governance

From 1 January 2019, the Financial Reporting Council's (FRC's) revised UK Corporate Governance Code (the Code) came into effect. According to the Code, the board should establish procedures to manage risk, oversee the internal control framework, and determine the nature and extent of the principal risks the company is willing to take in order to achieve its long-term strategic objectives.

Furthermore, the Code states, under the "comply or explain" mechanism, that listed companies should establish an audit committee that on behalf of the board is charged with overseeing the above process.

The Code highlights that one key role of the audit committee is to monitor and review the effectiveness of the company's internal audit function or, where there is none, consider annually whether there is a need for one and making a recommendation to the board.

In addition, the Code highlights that corporate culture is an important consideration in the governance of organisations. The revised Code highlights the key role for the board in establishing, promoting, assessing and monitoring the desired corporate culture. The focus on culture needs to be continuous. Periodic reflection on whether the culture continues to be relevant in a changing environment can help the company adapt its culture to ensure it continues to support the company's success. The board is expected to assess and monitor culture for alignment with purpose and values. Monitoring culture will involve regular analysis and interpretation of evidence and information gathered from a range of sources. Drawing insight from multiple quantitative and qualitative sources helps guard against forming views based on incomplete or limited information. The workforce will be a vital source of insight into the culture of the company.

The board needs to ensure these values are communicated by management, incentivising the desired behaviours and sanctioning inappropriate behaviour, and must assess whether the desired values and behaviours have become embedded at all levels.

The positioning and reach of internal audit and the ability to 'tell it how it is' are as important as the ability to audit cultural issues. Internal audit's role as the inside-outsider is the key to success when providing culture assurance.

However, internal audit should not be the sole provider on assurance on culture for boards. In conjunction with other departments, including human resources, risk and compliance, an integrated approach can provide a holistic view of an organisation's culture and how it impacts behaviours and performance.

The Wates Corporate Governance Principles for Large Private Companies say that those companies must report on how they are implementing and managing internal controls, which is an intrinsic element of good corporate governance – bringing them more in line with publicly-listed businesses. All companies with more than 2000 employees with a turnover of over £200 million and a balance sheet of over £2 billion need to report on their corporate governance arrangements – section 172 of *The Companies (Miscellaneous Reporting) Regulations 2018 Act*. These enterprises may need or find they are likely to benefit from internal audit.

APPENDIX TWO

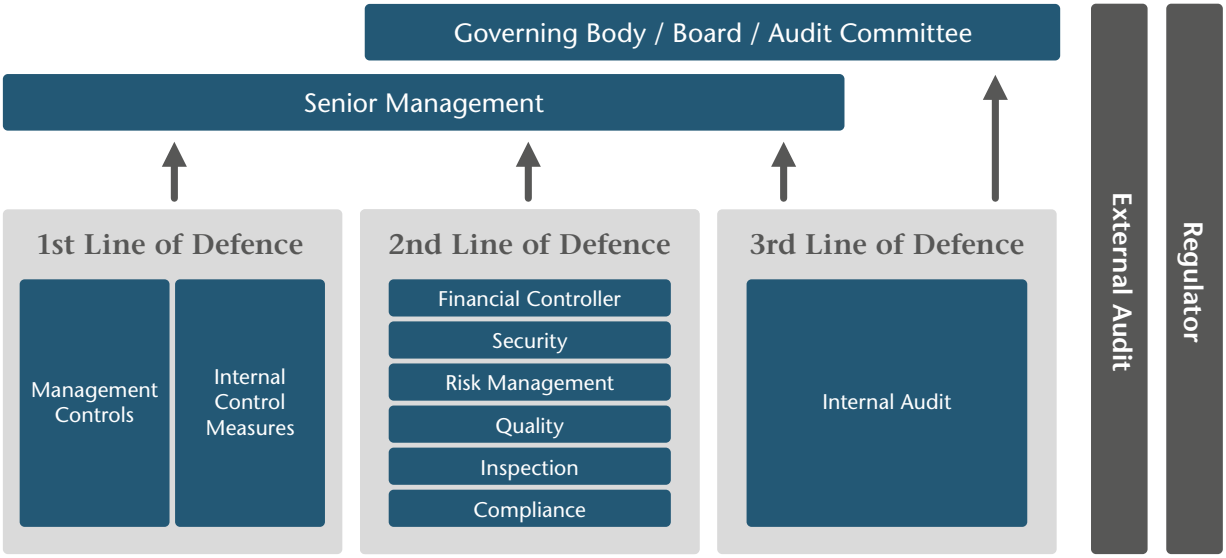
Internal audit and the governance of risk – the three lines of defence

The Chartered IIA and the IoD endorse the "three lines of defence" model as a way of explaining the risk governance of the business. The three lines of risk defence are:

1. the first line of defence – functions that own and manage risk;
2. the second line of defence – functions that oversee or specialise in risk management, compliance, etc. and
3. the third line of defence –internal audit.

Internal audit is uniquely positioned within the organisation to provide holistic assurance to the audit committee and senior management on the effectiveness of internal controls, governance and risk management. It is also well-placed to fulfil an advisory role on the coordination of assurance, effective ways of improving existing processes, and assisting management in implementing recommended improvements. In such a framework, internal audit is a cornerstone of an organisation's corporate governance.

The Three Lines of Defence Model



Adapted from ECII/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

Advisory Panel

The publication of *Harnessing the Power of Internal Audit* was made possible thanks to the advice and guidance of an advisory panel of corporate governance experts, who generously offered their time to attend meetings and provide comments on drafts of the thinkpiece. Whilst we must make clear that the panel members are not responsible for the contents of the final document, we would like to acknowledge and thank them for providing us with their valuable thoughts, insights and expertise.

MEMBERS OF THE PANEL INCLUDED:

- Mike Ashley, Audit Committee Chair, Barclays Plc
- Paul Boyle OBE, Chairman, Protect
- Professor Andrew Chambers, Author of Chambers' Corporate Governance Handbook
- Philippa Foster Back CBE, Director, Institute for Business Ethics
- Mary Hardy, Audit Committee Chair, Royal Navy
- Dr Roger Barker, Head of Corporate Governance, Institute of Directors
- Dr Ian Peters MBE, Chief Executive, Chartered Institute of Internal Auditors

About the Chartered IIA

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. About 2,500 members are Chartered Internal Auditors and have earned the designation CMIIA. Over 1,000 of our members hold the position of head of internal audit and the majority of FTSE 100 companies are represented amongst our membership.

Members are part of a global network of 180,000 members in 170 countries, all working to the same International Standards and Code of Ethics.

iia.org.uk

Chartered Institute of Internal Auditors

13 Abbeville Mews
88 Clapham Park Road
London SW4 7BX

Tel: 020 7498 0101
Email: info@iia.org.uk

Chartered Institute of Internal Auditors

The Institute of Directors

The IoD has been supporting businesses and the people who run them since 1903. As the UK's longest running and leading business organisation, the IoD is dedicated to supporting its members, encouraging entrepreneurial activity, and promoting responsible business practice for the benefit of the business community and society as a whole.

iod.com

The Institute of Directors

116 Pall Mall
London
SW1Y 5ED

Tel: 020 7451 3282
Email: policy-unit@iod.com

IoD *Inspiring* **business**