



# On the 2024 audit committee agenda

## KPMG Board Leadership Centre

**The business and risk environment has changed dramatically over the past year, with greater geopolitical instability, surging inflation, high interest rates, and unprecedented levels of disruption and uncertainty. Audit committees can expect their company's financial reporting, compliance, risk, and internal control environment to be put to the test by an array of challenges – from global economic volatility and the wars in Ukraine and the Middle East to cybersecurity risks and ransomware attacks and preparations for climate and sustainability reporting requirements, which will require developing related internal controls and disclosure controls and procedures. This is compounded by uncertainty in the UK regulatory landscape and in particular the extent to which internal control frameworks will need to be strengthened, evidenced and assured as a result of the on-going UK governance and audit reforms.**

Drawing on insights from our interactions with audit committees and business leaders, we've highlighted nine issues to keep in mind as audit committees consider and carry out their 2024 agendas

### **Stay focused on financial reporting and related internal control risks – job number one**

Focusing on the financial reporting, accounting, and disclosure obligations posed by the current geopolitical, macroeconomic, and risk landscape will be a top priority and major undertaking for audit committees in 2024. Key areas of focus should include:

#### **Forecasting and disclosures**

Among the matters requiring the audit committee's attention: Disclosures regarding the impact of the wars in Ukraine and the Middle East, government sanctions, supply chain disruptions, heightened cybersecurity risk, climate change, inflation, interest rates, market volatility, and the risk of a global recession; preparation of forward-looking cash-flow estimates; impairment of non-financial assets, including goodwill and other intangible assets; the impact of events and trends on liquidity; accounting for financial assets (fair value); going concern; and use of non-GAAP metrics.

With companies making more tough calls in the current environment, regulators are emphasising the importance of well-reasoned judgments and transparency, including contemporaneous documentation to demonstrate that the company applied a rigorous process. Given the fluid nature of the long-term environment, disclosure of changes in judgments, estimates, and controls may be required more frequently.

In reviewing management's disclosures regarding these matters, pay particular regard to the matters raised in the FRC's recent [Annual Review of Corporate Reporting](#).

#### **Internal control over financial reporting (ICOFR) and probing control deficiencies**

Notwithstanding the proposed changes to the UK Corporate Governance Code and the anticipated board declaration on the effectiveness of all material controls (see later), the current geopolitical, macroeconomic, and risk environment, as well as changes in the business, such as acquisitions, new lines of business, digital transformations, etc., internal controls will continue to put ICOFR to the test. Discuss with management how the current environment and regulatory mandates – including new climate rules – affect management's disclosure controls and procedures and ICOFR, as well as management's assessment of the effectiveness of ICOFR.

Probe any control deficiencies identified and help provide a balanced evaluation of the deficiency's severity and cause. Is the audit committee – with management – regularly taking a fresh look at the company's control environment? Have controls kept pace with the company's operations, business model, and changing risk profile, including cybersecurity risks? Does management talk the talk *and* walk the walk?

#### **Importance of a comprehensive risk assessment**

The importance of comprehensive risk assessment should not be underestimated. Help ensure that management and auditors are not too narrowly focused on information and risks that directly impact financial reporting while disregarding broader, entity-level issues that may also impact financial reporting and internal controls.

## Committee bandwidth and skillsets

The audit committee's role in overseeing management's preparations for new climate and sustainability reporting requirements further expands the committee's oversight responsibilities beyond its core oversight responsibilities (financial reporting and related internal controls, and internal and external auditors). This expansion should heighten concerns about audit committee bandwidth and 'agenda overload.'

Reassess whether the committee has the time and expertise to oversee the major risks on its plate today. Such a reassessment is sometimes done in connection with an overall reassessment of issues assigned to each board standing committee. For example, do cybersecurity, climate, ESG, or 'mission-critical' risks such as safety, as well as artificial intelligence (AI), including generative AI, require more attention at the full-board level – or perhaps the focus of a separate board committee? The pros and cons of creating an additional committee should be weighed carefully, but considering whether a finance, technology, risk, climate/sustainability, or other committee – and perhaps the need for directors with new skill sets – would improve the board's effectiveness can be a healthy part of the risk oversight discussion.

In reviewing management's disclosures regarding these matters, pay particular regard to the matters raised in the FRC's recent [Annual Review of Corporate Reporting 2022/23](#).

## Keep abreast of the audit reform agenda and encourage any necessary 'no regret' actions

The anticipated governance and audit reforms have stalled in late 2023. First, the Government withdrew the draft Regulation that would have required certain companies to prepare an annual resilience statement, disclosures relating to distributable profits and distributions, a material fraud statement, and a triennial audit and assurance policy statement. Then, as the Audit Bill did not feature in the Kings Speech on 7 November, we are unlikely to see any primary legislation to establish the Audit, Reporting and Governance Authority (ARGA) until after the General Election (which must take place before late January 2025 and is expected to happen in 2024).

Nevertheless, the FRC are still expected to issue a revised UK Corporate Governance Code in January 2024 and the main substantive revision will focus on internal controls. While the FRC's approach may depart from the "*much more intrusive approach adopted in the US*", this will still be an issue for audit committees to think about and prepare for.

What 'no regret' actions can organisations take now to ensure a smooth transition to any new framework? How will you oversee any necessary cultural shift? Are the benefits of any changes clearly articulated? How can technology be best leveraged? Is there agreement as to the organisation's principal risks starting with the key risks with a financial statement impact? If you don't know where your principal risks are you will end up with the wrong control environment.

## Maintain focus on cybersecurity and data privacy

Cybersecurity risk continues to intensify. The acceleration of AI, the increasing sophistication of attacks, the wars in Ukraine and the Middle East, and ill-defined lines of responsibility – among users, companies, vendors, and government agencies – have elevated cybersecurity risk and its place on board and committee agendas.

The growing sophistication of the cyber threat points to the continued cybersecurity challenge – and the need for management teams and boards to continue to focus on resilience. Breaches and cyber incidents are going to happen, and organisations must be prepared to respond appropriately when they do. In other words, it's not a matter of if, but when.

Regulators and investors are demanding transparency into how companies are assessing and managing cyber risk and building and maintaining resilience. For example, the SEC now require public companies to disclose material "cybersecurity incidents" within four business days.

While data governance overlaps with cybersecurity, it's broader and includes compliance with industry-specific laws and regulations, as well as privacy laws and regulations that govern how personal data – from customers, employees, or vendors – is processed, stored, collected, and used. Data governance also includes policies and protocols regarding data ethics – in particular, managing the tension between how the company may use customer data in a legally permissible way and customer expectations as to how their data will be used.

Managing this tension poses significant reputation and trust risks for companies and represents a critical challenge for leadership. How robust and up to date is management's data governance framework? Does it address third-party cybersecurity and data governance risks?

Cyber threats should be considered as part of the company's risk management process, and the audit committee should test whether the company has:

- Identified the critical information assets which it wishes to protect against cyber attack – the crown jewels of the firm – whether financial data, operational data, employee data, customer data or intellectual property.
- Intelligence processes in place to understand the threat to the company's assets, including their overseas operations.
- A way of identifying and agreeing the level of risk of cyber attack that the company is prepared to tolerate for a given information asset.
- Controls in place to prepare, protect, detect and respond to a cyber attack – including the management of the consequences of a cyber security incident.
- A means of monitoring the effectiveness of their cyber security controls, including where appropriate, independently testing, reviewing and assuring such controls.

- A programme of continuous improvement, or where needed, transformation, to match the changing cyber threat – with appropriate performance indicators.

## Clarify roles ahead of new climate, sustainability, and other ESG disclosures – and oversee the quality and reliability of the underlying data

As discussed in On the 2024 board agenda, an important area of board focus and oversight will be management's efforts to prepare for dramatically increased climate and ESG disclosure requirements in the coming years.

While certain companies have been required to provide climate related financial disclosures in their 2023 Strategic Reports, boards should also be aware of the UK Sustainability Disclosure Standards (UK SDS) that will form the basis of any future requirements in UK legislation for companies to report on governance, strategy, risks and opportunities, and metrics relating to sustainability matters, including risks and opportunities arising from climate change.

The UK SDS will be based on the IFRS Sustainability Disclosure Standards issued by the International Sustainability Standards Board (ISSB), and the UK endorsed standards will divert from the global baseline only if necessary for UK specific matters.

Companies doing business in Europe are also assessing the potential effects of, and preparing to apply, the European Sustainability Reporting Standards (ESRSs) issued under the Corporate Sustainability Reporting Directive (CSRD) in the EU, and IFRS Sustainability Disclosure Standards issued by the ISSB. The standards – which are based in part on the Task Force on Climate-Related Financial Disclosures (TCFD) Framework and the Greenhouse Gas Protocol – are highly prescriptive and expansive. The CSRD also includes a requirement for large non-EU companies that operate in the EU to provide sustainability reporting.

Also, under the SEC's proposed climate disclosure rule, companies, including foreign registrants, will need to provide an account of their greenhouse gas (GHG) emissions, the environmental risks they face, and the measures they're taking in response. Crucially, according to the proposed rule, issuers will be subject to mandatory limited assurance initially, with mandatory reasonable assurance being phased in for accelerated and large accelerated filers. In addition, some information will need to be disclosed in the notes to the financial statements.

Companies will need to keep abreast of ongoing developments and determine which standards apply, and the level of interoperability of the applicable standards. For example, there are different materiality thresholds. The US and ISSB consider financial materiality — in which information is material if investors would consider it important in their decision-making — whereas the UK and EU use the concept of “double materiality”, through the lenses of the financial effect on the company and the impact the company has on the wider community and environment.

A key area of board and audit committee focus will be the state of the company's preparedness – requiring periodic updates on management's preparations, including gap analyses, materiality assessments, resources, assurance readiness and any new skills needed to meet regulatory deadlines.

In addition to the compliance challenge, companies must also ensure that disclosures are consistent, and consider the potential for liability posed by detailed disclosures.

This will be a major undertaking, with cross-functional management teams involved and multiple board committees overseeing different aspects of these efforts.

Given the scope of the effort, audit committees should encourage management to prepare now by assessing the path to compliance with applicable reporting standards and requirements – including the plan to develop high quality, reliable climate and sustainability data. Key areas of audit committee focus should include:

- Clarifying internal roles and responsibilities in connection with the disclosures in the annual report and accounts, other regulatory reports and those made voluntarily in sustainability reports, websites, etc. – including coordination between any cross-functional management ESG team(s) or committee(s).
- Ensuring management have processes in place to review the disclosures, including for consistency with the annual report and accounts. Making sure the teams looking at ESG issues/reporting are properly connected to the core finance function is important.
- Helping to ensure that ESG information being disclosed is subject to the same level of rigor as financial information – meaning disclosure controls and procedures. Given the nature of the climate, sustainability, and ESG reporting requirements and the intense focus on these disclosures generally, companies should consider enhancing management's disclosure processes to include appropriate climate, sustainability, and other ESG functional leaders, such as the ESG controller (if any), chief sustainability officer, chief human resources officer, chief diversity officer, chief supply chain officer, and chief information security officer.
- Encouraging management to identify any gaps in governance and consider how to gather and maintain quality information. Also, closely monitor UK and global rulemaking activities.
- Understanding whether appropriate systems are in place or are being developed to ensure the quality of data that must be assured by third parties.

## Reinforce audit quality

Audit quality is enhanced by a fully engaged audit committee that sets the tone and clear expectations for the external auditor and monitors auditor performance rigorously through frequent, quality communications and a robust performance assessment.

In setting expectations for 2024, audit committees should discuss with the auditor how the company's financial reporting and related internal control risks have changed in light of the geopolitical, macroeconomic, regulatory and risk landscape, as well as changes in the business.

Set clear expectations for frequent, open, candid communications between the auditor and the audit committee, beyond what's required. The list of required communications is extensive and includes matters about the auditor's independence as well as matters related to the planning and results of the audit.

Taking the conversation beyond what's required can enhance the audit committee's oversight, particularly regarding the company's culture, tone at the top, and the quality of talent in the finance organisation.

Audit committees should also probe the audit firm on its quality control systems that are intended to drive sustainable, improved audit quality – including the firm's implementation and use of new technologies such as AI to drive audit quality.

In discussions with the external auditor regarding the firm's internal quality control system, consider the results of recent regulatory inspections and internal inspections and efforts to address deficiencies. Remember that audit quality is a team effort, requiring the commitment and engagement of everyone involved in the process – the auditor, audit committee, internal audit, and management.

Looking more widely, ask are we 'doing the right thing?' Many companies are thinking about how they are perceived by shareholders and other stakeholders. This is empowering some audit committees to extend the independent (external) assurance they receive – whether from the external auditor or other third party assurance providers.

Our [2023 FTSE350 Audit Committee Chair Survey](#) revealed that the areas where audit committee chairs are most likely to seek assurance from their external auditor are the Directors' Remuneration Report, the effectiveness of internal controls over financial reporting (ICOFR), the KPIs associated with the 'E' in ESG, and TCFD reports.

Be cognisant of the capacity constraints within the audit profession. Think ahead if an audit tender is due or planned – getting the 'right' auditor may be more difficult than expected. With audit tenders typically being carried out two years ahead of the transition date, the time to plan, build relationships, and determine which firms should take part in the tender might need to start much earlier than first thought.

Finally, have regard to the FRC's 2023 'Audit Committees and the External Audit: Minimum Standard'. While the Standard is primarily aimed at audit committees within the FTSE350 and largely drawn from existing guidance and best practice, new text has been included to reflect the current focus on diversity in the audit market. Companies that are not within the FTSE 350 might still look to the Standard for examples of good practice.

## **Make sure internal audit is focused on the company's key risks and is a valuable resource to the audit committee**

As audit committees wrestle with heavy agendas – and risk management is put to the test – internal audit should be a valuable resource for the audit committee and a crucial voice on risk and control matters. This means focusing not just on financial reporting and compliance risks, but also critical operational and technology risks and related controls, as well as ESG risks.

ESG-related risks are rapidly evolving and include human capital management – from diversity, equity, and inclusion (DEI) to talent, leadership, and corporate culture – as well as climate, cybersecurity, data governance and data privacy, and risks associated with ESG disclosures. Disclosure controls and procedures and internal controls should be a key area of internal audit focus. Clarify internal audit's role in connection with ESG risks and enterprise risk management more generally – which is not to manage risk, but to provide added assurance regarding the adequacy of risk management processes. Do management teams have the necessary resources and skill sets to execute new climate and ESG initiatives?

Reassess whether the internal audit plan is risk-based and flexible enough to adjust to changing business and risk conditions. The audit committee should work with the head of internal audit and chief risk officer to help identify the risks that pose the greatest threat to the company's reputation, strategy, and operations, and to help ensure that internal audit is focused on these key risks and related controls.

These may include industry-specific, mission-critical, and regulatory risks, economic and geopolitical risks, the impact of climate change on the business, cybersecurity and data privacy, risks posed by generative AI and digital technologies, talent management and retention, hybrid work and organisational culture, supply chain and third-party risks, and the adequacy of business continuity and crisis management plans.

Given internal audit's broadening mandate, it will likely require upskilling, like the finance organisation. Set clear expectations and help ensure that internal audit has the talent, resources, skills, and expertise to succeed – and help the head of internal audit think through the impact of digital technologies on internal audit.

## **Maintain a sharp focus on leadership and talent in the finance organisation**

Finance organisations face a challenging environment today – addressing talent shortages, while at the same time managing digital strategies and transformations and developing robust systems and procedures to collect and maintain high-quality ESG data to meet both investor and other stakeholder demands. Many are contending with difficulties in forecasting and planning for an uncertain environment, and working with the workforce to ensure they remain motivated and engaged is becoming harder.

As audit committees monitor and help guide finance's progress in these areas, we suggest two areas of focus:

- Many finance organisations have been assembling or expanding management teams or committees charged with managing a range of ESG activities, including enhancing controls over the ESG information being disclosed in corporate reports. Does the finance organisation have the leadership, talent, skill sets, and other resources necessary to address climate and other ESG reporting and to ensure that quality data is being collected and maintained? Has adequate consideration been given to the diversity of the team and the pipeline? How far along is the finance organisation in its preparations for any new/enhanced ESG disclosures?
- At the same time, the acceleration of digital strategies and transformations, presents important opportunities for finance to add greater value to the business. The finance function is combining strong analytics and strategic capabilities with traditional financial reporting, accounting, and auditing skills.

It is essential that the audit committee devote adequate time to understanding finance's climate/sustainability/ESG strategy and digital transformation strategy and help ensure that finance is attracting, developing and retaining the leadership, talent, skill sets and bench strength to execute those strategies, as well as its existing responsibilities. Staffing deficiencies in the finance department may pose the risk of internal control deficiencies.

## Help sharpen the company's focus on ethics, compliance, and culture

The reputational costs of an ethics or compliance failure are higher than ever, particularly given increased fraud risk, pressures on management to meet financial targets, and increased vulnerability to cyberattacks.

Ensure management are prepared for the [Economic Crime and Corporate Transparency Act 2023](#) and in particular the new 'failure to prevent fraud' corporate criminal offence which will render large companies liable for fraud committed by their associates – including employees, agents, subsidiaries and persons who otherwise perform services for or on behalf of the organisation. Under the new regulations, prosecutors will no longer have to show that the 'directing mind and will' of a company were involved in the fraud.

Fundamental to an effective compliance program is the right tone at the top and culture throughout the organisation, including commitment to its stated values, ethics, and legal and regulatory compliance. This is particularly true in a complex business environment, as companies move quickly to innovate and capitalise on opportunities in new markets, leverage new technologies and data, engage with more vendors and third parties across complex supply chains.

Closely monitor the tone at the top and culture throughout the organisation with a sharp focus on behaviors (not just results) and yellow flags. Is senior management sensitive to ongoing pressures on employees (both in the office and at home), employee health and safety, productivity, and employee engagement and morale? Leadership, communication, understanding, and compassion are essential. Does the company's culture make it safe for people to do the right thing? It is helpful for directors to spend time in the field meeting employees to get a better feel for the culture. Help ensure that the company's regulatory compliance and monitoring programs are up to date, cover all vendors in the global supply chain, and communicate the company's expectations for high ethical standards.

Focus on the effectiveness of the company's whistleblower reporting channels (including whether complaints are being submitted) and investigation processes.

Does the audit committee see all whistle-blower complaints? If not, what is the process to filter complaints that are ultimately reported to the audit committee? With the radical transparency enabled by social media, the company's culture and values, commitment to integrity and legal compliance, and its brand reputation are on full display.

## Clarify oversight of generative AI

As discussed in 'On the 2024 board agenda', oversight of generative AI will be an oversight priority for almost every board in 2024.

Like ESG, the oversight of generative AI may touch multiple committees and the audit committee may end up overseeing compliance with the patchwork of differing laws and regulations governing generative AI, as well as the development and maintenance of related internal controls and disclosure controls and procedures.

Some audit committees may have broader oversight responsibilities for generative AI, including oversight of various aspects of the company's governance structure for the development and use of the technology.

How and when is a generative AI system or model – including a third-party model – developed and deployed, and who makes that decision? What generative AI risk management framework is used? Does the organisation have the necessary generative AI-related talent and resources?

Given how fluid the situation is – with generative AI gaining rapid momentum – the allocation of these oversight responsibilities to the audit committee may need to be revisited throughout the year.

---

## The KPMG Board Leadership Centre

The KPMG Board Leadership Centre offers support and guidance to non-executive directors, whether managing a portfolio non-executive career or embarking on a first appointment. Membership offers you a place within a community of board-level peers with access to topical and relevant seminars, invaluable resources and thought leadership, as well as lively and engaging networking opportunities. We equip you with the tools you need to be highly effective in your role, enabling you to focus on the issues that really matter to you and your business.

Learn more at [www.kpmg.com/uk/blc](http://www.kpmg.com/uk/blc).

## Contact us

**Timothy Copnell**

Board Leadership Centre

**T:** +44 (0)20 7694 8082

**E:** [tim.copnell@kpmg.co.uk](mailto:tim.copnell@kpmg.co.uk)

[www.kpmg.com/uk/blc](http://www.kpmg.com/uk/blc)



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2023 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.