On the 2024 audit committee agenda

KPMG Nigeria Board Governance Centre

February 2024

The business and risk environment has changed dramatically over the past year, with greater geopolitical instability, surging inflation, high interest rates, 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 to cybersecurity risks and ransomware attacks, digital disruption, talent management and retention as well as preparations for compliance with the Financial Reporting Council (FRC) Amendment Act.

Drawing on insights from our interactions with audit committees and business leaders, we've highlighted eight issues for audit committees to keep in mind as they 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 increase in fuel price, policy uncertainty, challenges related to foreign exchange availability, currency devaluation, supply chain disruptions, cybersecurity risk, climate change, inflation, interest rates, market volatility, and the risk of a global recession. Additionally, the committee should oversee the preparation of forward-looking cash-flow estimates, assess the impairment of non-financial assets such as goodwill and intangible assets, evaluate the impact of events and trends on liquidity, review the accounting treatment for financial assets, particularly their fair value, and consider matters related to the organisation's going concern.

As businesses navigate challenges in the current environment, regulators are emphasising the importance of making well-founded decisions and maintaining transparency. This includes the need for contemporaneous documentation to demonstrate that the company applied a thorough and rigorous decision-making process.

Due to the dynamic nature of the long-term business landscape, there might be a heightened necessity for more frequent disclosure regarding changes in judgments, estimates, and controls.

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

Reflecting on the current geopolitical, macroeconomic, and risk environment, as well as changes in the business, such as acquisitions, new lines of business, digital transformations, etc., the effectiveness of internal controls over financial reporting (ICOFR) will face ongoing scrutiny and challenges.

Discuss with management on how the current environment and regulatory mandates – including the Financial Reporting Council (FRC) Amendment Act – impact businesses. The Act aims to make financial reporting more reliable, increase transparency in corporate disclosures, build confidence among investors, and promote sustainable development. With the FRC expecting compliance with the Amended Act in 2024, it is important to keep an eye on how management is geared towards compliance with the FRC amendment Act.

Additionally, there is a need to discuss with management how they evaluate the effectiveness of ICOFR, probe any control deficiencies identified and help provide a balanced evaluation of the deficiency's severity and cause. The

key questions the audit committee should ask here are: Is the audit committee together with management, regularly taking a fresh look at the company's control environment? Have financial 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 significance of a comprehensive risk assessment should not be overlooked. Assist in ensuring that both management and auditors maintain a broad perspective, addressing not only specific information and risks directly impacting financial reporting but also considering overarching entity-level issues that can affect both 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, Environment, Social and Governance (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.

Maintain focus on cybersecurity and data privacy

Cybersecurity risk continues to intensify. The acceleration of AI, the increasing sophistication of attacks, 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.

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.

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. The key questions the audit committee should ask here are: How robust and up to date is management's data governance framework? Does it address third-party cybersecurity and data governance risks?

Be prepared to oversee sustainability and climate change matters including their disclosure and the quality of the underlying data

As discussed, 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/sustainability disclosure requirements for companies in the coming years.

Boards should stay informed about the recent regulations, standards, and guidelines related to ESG, such as the Nigerian Climate Change Act, and the IFRS S1 and S2 Standards issued by the International Sustainability Standards Board (ISSB). Nigeria is one

of the early adopters as announced in June 2023 by the Financial Reporting Council (FRC) and the Nigeria Exchange Group Regulation Limited (NGX). Consequently, 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, assurance readiness, adequacy of resources and any new skills needed to meet regulatory deadlines and assurance readiness.

In addition to the compliance challenge, companies must also ensure that disclosures are consistent and accurate, while considering the potential for liability posed by greenwashing.

This will be a major undertaking, with cross-functional management teams involved, multiple board committees overseeing different aspects of these efforts including several training and awareness sessions to ensure proper understanding of the standards..

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 sustainability and climate change 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 has processes in place to review the disclosures, including reviews for consistency with the annual report and accounts. Making sure the teams responsible for ESG matters/ reporting are well connected to the core finance function is important.
- Helping to ensure that ESG information being disclosed is subject to the same level of rigour as financial information – meaning disclosure controls and procedures. Given the nature of the sustainability/ESG and climate change 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 functional leaders who have a role to play in ESG management, such as the Head Sustainability/ 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.
- Understanding whether appropriate systems are in place or are being developed to ensure the quality of ESG 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.

Ensure internal audit is focused on the company's key risks and is a valuable resource to the audit committee

In the face of demanding agendas for audit committees and heightened challenges in risk management, internal audit should serve as a valuable asset to the audit committee, providing an essential voice on matters pertaining to risk and control. This implies directing attention not only to financial reporting and compliance risks but also to critical operational and technology risks including their related controls, as well as ESG risks.

ESG-related risks are dynamic and rapidly evolving, encompassing aspects such as human capital management, leadership, corporate culture, climate, cybersecurity, data governance, data privacy, and risks linked to ESG disclosures. Disclosure controls and procedures and internal controls should be a key area of internal audit focus. Audit committee should 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. With the tight labour market and the increased resignation rate, does the internal audit function have the necessary resources and skill sets? Recognise that internal audit is not immune to these talent pressures.

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, cybersecurity and data privacy, risks posed by 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. Audit committee should 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

TFinance 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 business control 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 potential damage to reputation resulting from an ethics or compliance failure is now more significant than ever. This is particularly true due to heightened fraud risks, pressures on management to achieve financial targets, and increased susceptibility to cyberattacks.

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? Directors can gain valuable insights into the culture by spending time in the field and engaging with employees directly.

Assist in verifying that the company's regulatory compliance and monitoring programs are current, encompassing all vendors across the global supply chain, and effectively communicate the company's expectations regarding high ethical standards.

Give attention to the efficiency of the company's whistleblower reporting channels, evaluating factors such as the submission of complaints, and assessing the effectiveness of the 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

Define the audit committee's oversight responsibilities for 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.

About the KPMG Board Governance Centre

The KPMG Board Governance Centre (BGC) is a dedicated forum that provides Board members with insights and resources to keep abreast of current and emerging governance issues.

The KPMG BGC offer thought leadership and timely resources including periodic seminars and round tables to host the exchange of views and support Board members (including Board sub-committee members) in clarifying and enhancing their governance practices amid rapidly evolving corporate governance landscape in Nigeria.

Learn more: http://bit.ly/board-governance-centre

Contact us

Tomi Adepoju
Partner & Head,
Board Governance and
ESG, Advisory Services
KPMG in Nigeria
E: tomi.adepoju@ng.kpmg.com

Tolu Odukale
Partner & Head,
Internal Audit, Governance,
Risk & Compliance Services
KPMG in Nigeria
E: tolulope.odukale@ng.kpmg.com

Bimpe Afolabi
Partner,
Internal Audit, Governance,
Risk & Compliance Services
KPMG in Nigeria
E: bimpe.afolabi@ng.kpmg.com

home.kpmg/ng
home.kpmg/socialmedia