KPMG

On the audit committee agenda 2025

Board Leadership Center (India)

KPMG. Make the Difference.

Introduction

An Audit Committee (AC) can expect its company's financial reporting, compliance, risk, and internal control environment to be put to the test in 2025 by an array of challenges that have grown and intensified over the past year. From global economic volatility and the wars, to cyberattacks, to preparations related to climate and sustainability reporting requirements, and advances in Artificial Intelligence (AI). In this volatile and opaque operating environment, demands by regulators, investors, and other stakeholders for more action and greater disclosure and transparency – is expected to intensify and the range and interconnectedness of risks and macro forces are putting corporate governance to the test. The role of an AC is of paramount importance, considering the need for robust corporate governance.

Due to the developments that have taken place in the regulatory and legal environment, the AC members should be mindful of certain critical amendments having an impact in the upcoming year for which necessary processes should be in place.

Drawing on insights from our interactions with ACs and business leaders, we have highlighted the following six issues to keep in mind as ACs consider and conduct their 2025 agendas.

01 Keeping pace with accounting, auditing and regulatory developments

Corporate reporting in India continues to evolve, with both investors and regulators playing a role in shaping the reporting landscape in the country. In order to keep pace with the evolving regulatory mandates and far-reaching expectations of the stakeholders, it has become imperative for the AC to keep the finger on the pulse of developments in the recent reporting requirements.

Related Party Transactions (RPTs)

The Companies Act, 2013 (2013 Act) and the Securities and Exchange Board of India (SEBI) (Listing Obligations and Disclosure Requirements) Regulations, 2015 (Listing Regulations) require AC approval for all Related Party Transactions (RPTs). To simplify compliance, SEBI has introduced amendments that exclude certain corporate actions and transactions, exempt remuneration and sitting fees for non-promoter directors, and allow independent directors to ratify certain RPTs. Additionally, the AC can now grant omnibus approval for RPTs by subsidiaries, and specific transactions involving public sector companies and government payments are exempt from approval. The Industry Standards Forum (ISF) has also issued standards to apply uniform format of information that ACs and shareholders can evaluate for thorough assessment before approval. These standards were made effective for RPTs on or after 1 April 2025. . However, on 21 March 2025, SEBI clarified that on the basis of feedback from various stakeholders, the effective date would be 1 July 2025.

Ease of doing business amendments to SEBI Listing Regulations

The recent amendments to the SEBI Listing Regulations aim to enhance the ease of doing business by streamlining disclosure requirements and improving transparency. Key changes include the requirement for listed entities to disclose material events within three hours of a board meeting closure if it occurs after normal trading hours and extending the timeline for disclosing litigations or disputes to 72 hours. Tax litigations must be disclosed within 24 hours of receipt, with quarterly updates to be provided. The threshold for disclosing changes in shareholding percentages has been increased, and fraud reporting by senior management is now limited to instances related to the listed entity. Additionally, a single filing system has been implemented, and an integrated filing system for periodic filings has been introduced. Other amendments include obligations on promoters, directors, and Key Managerial Personnels (KMPs) to disclose relevant information, changes in terminology for identifying material subsidiaries, and new requirements for board committee vacancies and independent director meetings. These amendments are designed to ensure compliance with applicable laws and improve corporate governance.

BRSR updates

To facilitate ease of doing business for listed entities and their value chain partners regarding Environmental, Social and Governance (ESG) disclosures and assurance under the Business Responsibility and Sustainability Report (BRSR), several amendments have been issued. These include the substitution of the term 'assurance' with 'assessment or assurance' under SEBI Listing Regulations, applicable from FY 2024-25. The ESG disclosures for the value chain and their assessment or assurance have been deferred by one year, making them applicable from FY 2025-26 and FY 2026-27, respectively. Voluntary ESG disclosures for FY 2024-25 will replace the 'comply-and-explain' requirement. The scope of the value chain has been clarified to cover top upstream and downstream partners, with an option to limit disclosure to 75 per cent of its purchases and sales. Additionally, the ISF has developed Industry Standards to help listed entities comply with BRSR Core disclosures, applicable from FY 2024-25 onwards.

Audit trail considerations

Effective from 1 April 2023, every company is required to incorporate the feature of audit trail in its accounting software used to maintain its books of accounts. Further, an auditor is required to include his/her views and comments in the audit report whether a company has used such an accounting software for maintaining its books of account which has a feature of recording audit trail (edit log) facility. An auditor should also comment on whether the audit trail feature has been operated throughout the year for all transactions recorded in the software and the audit trail feature has not been tampered with.

Fraud risk management framework for banks and NBFCs

In July 2024, the Reserve Bank of India (RBI) issued three revised master directions on fraud risk management applicable to banks, Non-Banking Financial Companies (NBFCs), including Housing Finance Companies (HFCs), and co-operative banks. These directions provide a robust framework for the prevention, early detection, and timely reporting of frauds in Regulated Entities (REs). The scope has been extended to Regional Rural Banks and all NBFCs with an asset size of INR500 crore and above. For the first time, governance requirements have been prescribed for NBFCs, while banks are required to follow a more structured approach. The revised directions also include a framework for Early Warning Signals (EWS) for fraud detection, defined roles for internal audits, and new requirements for legal audits of large value loan accounts. Additionally, REs must report fraud incidents to Law Enforcement Agencies (LEAs) within a prescribed timeline and disclose frauds as per the new guidelines.

Areas of focus

- Independent directors should ensure continuous review and evaluation of RPTs. Evaluating the procedures and processes for classification of related parties and RPTs helps with right identification and justification for RPTs and would also ensure correct and timely approvals
- The relaxation related to AC approvals has been provided by SEBI, however, similar exemptions not provided by the `t, therefore considering inconsistency, the transactions (as specified above) would continue to require approvals of the AC
- The Industry Standards on BRSR Core reporting provides definitions for various terms and aim to bring consistency of disclosures by reporting entities. The ACs along with the listed entities should assess FY 2024 approach against the Industry Standards guidance to identify areas needing re-computation. The guidance on what third party assessment would comprise is awaited
- Ensure management has implemented specific processes and controls over maintenance and monitoring of audit trail in respect of books of account, to demonstrate that audit trail was operating effectively throughout the period of reporting
- Ensure existence of periodic review mechanism and it is operating effectively for any changes to the audit trail configuration.

Questions for the audit committee to consider

1. Has the management have a clear and structured process for the identification and implementation of latest financial reporting and compliance requirements? The key focus areas being amendments to SEBI Listing Regulations, RPT amendments, implementation of audit trail, etc?
2. Has the management discussed the potential impact of the financial reporting and compliance changes with the auditors and Those Charged with Governance (TCWG)?
3. Does the management implement proper systems, controls and processes to ensure appropriate capture, sufficient approvals and timely disclosure of RPTs? How frequently does the management review the policy on materiality of RPTs?
4. Do the disclosures provided to the AC and shareholders regarding justification of an RPT comply with the spirit of the law and provide relevant and detailed information to enable them for taking an informed decision? Has the management initiated the process to implement the requirements of industry standards on RPTs?
5. Has the management reviewed the disclosures, ensured consistency and quality of the data disclosed in its BRSR (forming part of the annual report and financial statements)? Is management monitoring ESG information included within the annual report with the same rigour as conventional financial data?

02 Clarify the role of the AC in the oversight of technological development and data governance

Technology automation within the finance function provides greater insights, reduces the time of repetitive activities, results in efficiency and enables management to focus on the core activities that result in business value enhancements. There are numerous software tools and techniques available to assist organisations, such as cloud computing, robotic process automation, process mining, machine learning, artificial intelligence and bigdata. New technologies are also exposing organisations to new and emerging risks in addition to creating countless opportunities. Considering emerging risks, organisations should strive to identify, manage and monitor these risks. Some organisations are utilising Generative AI (GenAI) and establishing policies to protect against associated risks such as reputational and regulatory risks.

For many companies, much of the board's oversight responsibility for cybersecurity and data governance has resided with the AC. With the explosive growth in GenAI and the significant risks posed by the technology, boards are rigorously assessing their data governance and cybersecurity frameworks and processes.

Areas of focus

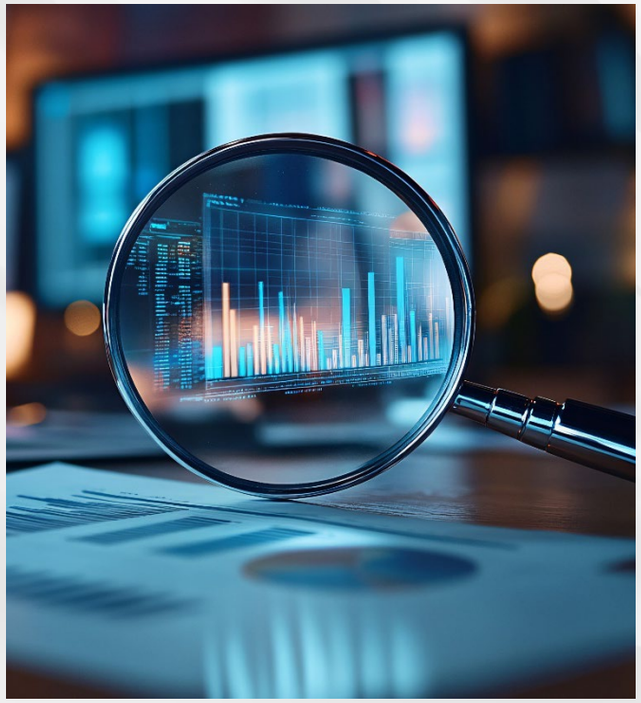
- Organisations need to determine the potential value of GenAI across their enterprise through the lens of workforce capacity and productivity. Identifying and recruiting individuals with relevant talent and expertise is critical for organisations
- ACs should allocate sufficient time to understand the finance organisation's GenAI and digital transformation strategy. ACs should also ensure that the finance department is attracting, developing, and retaining the necessary leadership, talent, skills, and bench strength to execute these strategies alongside its existing responsibilities. Any staffing deficiencies in the finance department could lead to an internal control deficiency, including a material weakness
- Apart from finance function, ACs should understand the use of AI and other digital transformations in audit functions and satisfy themselves that management and auditors know how it's being employed. ACs may ask management to establish a framework for assessing the effectiveness of AI and other technologies deployment including attaching Key Performance Indicators (KPIs) to these assessments. These KPIs should be reported to the AC regularly, and AI should be a regular agenda item at committee meetings
- ACs have a critical role to play in ensuring that their organisations have robust cyber security defences – not in understanding the specifics of the technology involved, but in leading governance and policy. This may require education or even bringing news skills into the boardroom and ACs. Given the AC's heavy agenda, the board may also seek to have another board committee or sub-committee under AC to do the heavy lifting on cybersecurity and data governance.

Questions for the audit committee to consider

1. How is management or the organisation identifying and addressing new risks being introduced with AI and GenAI?
2. How is management ensuring that its employees, management and board members are properly educated and trained in the technology solutions being deployed?
3. How does management ensure that its AI network and its data protection strategy is in alignment with the guiding principles of current applicable regulatory framework?
4. What precautions management taking to ensure that when GenAI is used to access data, it provides only the necessary data and only to authorised users?
5. How and when is a GenAI system or model including a third-party model developed and deployed, and who makes that decision? Understand GenAI risk management framework used by the company?
6. Evaluate whether coverage of the cyber insurance policy of the company is adequate to compensate in case of a cyber-security incident?
7. Does the company evaluate what is the company's diligence of cyber defence and what are the appropriate response and recovery mechanism from such cyber incidents? Has the company hired/invested in talented cyber-security professionals to manage cyber-security risks?

03 Ensure internal audit is focussed on company's key risks and is a valuable resource to the AC

Internal audit is a valuable resource for the AC and a crucial voice on risks and control matters. AC should renew the scope, staffing and budget of the internal audit function and holding executive session with the internal audit function.



Areas of focus

- Internal audit's broadening mandate might require upskilling the function. Set clear expectations and help ensure that internal audit has the talent, resources, skills, and expertise to succeed—and help the chief audit executive think through the impact of digital technologies on internal audit
- Controls and procedures should be a key area of internal audit focus. Clarify internal audit's role in connection with emerging risks such as ESG risks and enterprise risk management which is not to manage risk, but to provide added assurance regarding the adequacy of risk management processes
- Given the evolving geopolitical, macroeconomic, and risk landscape, reassess whether the internal audit plan is risk-based and flexible enough to adjust to changing business and risk conditions. AC 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 focussed on these key risks and related controls.

Questions for the audit committee to consider

1. Is there identified and assigned responsibility in the business for analysing, monitoring and interpreting geopolitical events?
2. Has the company conducted stress test on financial forecasts and business plans for geopolitical disruptions?
3. What are the risks posed by the company's digital transformation and by the company's extended organisation – sourcing, outsourcing, sales, and distribution channels?
4. Has the organisation ensure that the role and responsibilities of internal audit team are clearly outlined in the terms of reference and regularly review it to incorporate changes aligned to the business, risks and control environment?
5. In case of in-house internal audit function, do management teams have the necessary resources, and skill sets to address new risks and initiatives? How does management ensure upskilling of the internal audit team and ensure adequate talent, resources and skills within the department?
6. Is the coverage of internal audit adequate including periodicity, geography, locations, sites, business units, etc.?

04 Stay focussed on audit quality and stay abreast of the 'assurance challenge'

Recent regulatory scrutiny has emphasised both the fundamental role of ACs in effective stewardship and the importance of an effective, high quality, statutory audit. It is fundamentally important that the auditor approaches the audit with adequate professional skepticism and challenge. The AC should contribute to the enhancement of audit quality by setting a tone with management that supports open and robust challenge. Delivering a high-quality audit relies on the auditor, management and TCWG (boards and their ACs) working effectively together.

Furthermore, regulators continue to focus on the quality of corporate reporting by reviewing the financial statements and audit reports to ensure compliance with applicable laws and regulations and also corroborate filings made by companies both within India and internationally. These regulators have enhanced their supervision and have been issuing observations to highlight the instances of non-compliances with respect to financial reporting requirements such as Ind AS, Standards on Auditing, Schedule III to the Companies Act, 2013, Companies (Auditor's Report) Order, 2020 (CARO), etc. The learnings from the regulatory scrutiny and inspections contribute to strong reporting and oversight ecosystem and also helps ACs to identify the root cause of audit issues and continuously help improve audit quality.

Areas of focus

- Ensure an effective oversight on the appointment and re-appointment decisions of the external auditor with enhanced focus on auditor independence
- Focus on enhancing audit quality through effective and clear communication with the external auditor and a robust performance assessment. Set clear expectations for frequent, open, candid communications between the auditor and the AC, beyond the required communications that include matters about the auditor's independence as well as matters related to the planning and results of the audit
- ACs 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. The effectiveness and value of the audit should keep improving over time particularly as technology enables auditors to test large populations of data and provide enhanced business insights
- ACs should look out for the review reports issued by various bodies such as the National Financial Reporting Authority (NFRA), the Financial Reporting Review Board (FRRB), Quality Review Board (QRB), SEBI, overseas regulators, etc. and should understand the implications of the inspection reports on the company. Audit quality is a combined responsibility, requiring the commitment and engagement of everyone involved in the process –the auditor, AC, and management. The AC while discussing with auditors should consider the results of regulatory inspections and internal inspections and efforts to address deficiencies.

Questions for the audit committee to consider

1. Has an appropriate discussion taken place with the external auditor regarding major issues that arose during the course of the audit, the key accounting and auditing judgements and the level of errors identified during the audit?
2. Has the external auditor ensured sufficient and proportionate documentation for risk assessed areas of material importance?
3. Has the AC leveraged its work with internal audit function to ensure a high audit quality with the external auditor?
4. How ACs are looking at regulatory developments including international developments and analysing it from regulators' lens – NFRA, FRRB, ESMA findings, PCAOB[1] inspections etc?
5. What worked well in 2024, and what are the goals or milestones for improvements in 2025?

[1]National Financial Reporting Authority(NFRA), Financial Reporting Review Board (FRRB), European Securities and Markets Authority (ESMA) and Public Company Accounting Oversight Board (PCAOB)

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

A company's culture and ethics define the values and goals which help foster trust and loyalty amongst its stakeholders and establish a positive image and identity. The reputational costs of an ethics or compliance failure are higher than ever, increased fraud risk, pressures on management to meet financial targets, and increased vulnerability to cyber-attacks.

Fundamental to an effective compliance program is the right tone at the top and culture throughout the organisation, including its commitment to its stated values, ethics, and legal/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. 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. An AC should work towards creating an appropriate balance between strong relationships and robust oversight.

Areas of focus

- Closely monitor the tone at the top and culture throughout the organisation with a sharp focus on behaviors (not just results) and yellow flags. Leadership, communication, understanding, and compassion are essential. The company's culture make it safe for people to do the right thing. ACs to ensure to create a safe space to safeguard people to speak up when things aren't going right – because things do go wrong and it needs to be about how you are transparent about that and how you recover from it. Focus on the 'why' instead of 'what'. ACs should have meaningful discussion with the management to understand the cultural drivers and the root cause of misconduct
- Focus on the effectiveness of the company's whistleblower reporting channels (including whether complaints are being submitted) and investigation processes
- ACs should consider the radical exposure of the company's culture and values, commitment to integrity and legal compliance, and its brand reputation in this evolving digital age.

Questions for the audit committee to consider

1. Does the tone at the top emphasise antifraud culture throughout the company?
2. 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? Should the directors be spending more time in the field meeting employees to get a true picture of the culture within the organisation?
3. Have the whistle-blower complaints been resolved in time? Does the AC see all whistle-blower complaints? What is the process of filtering the whistleblower complaints that reach the AC?
4. In case of huge changes, how does the AC ensure they are getting sufficient visibility and that the right people are being held to account for delivering such change safely and effectively?

06 Focus on talent within the organisation and the AC

Finance teams face a challenging environment—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 climate and sustainability data both to meet investor and other stakeholder demands and in preparation for new disclosure requirements. At the same time, many are contending with difficulties in forecasting and planning for an uncertain environment.

Similarly, considering the continued expansion of the AC's oversight responsibilities beyond its core oversight responsibilities (financial reporting and related internal controls, and internal and external auditors) has heightened concerns about the committee's bandwidth, composition and skill sets. Therefore, the ACs are also required to assess on continuous basis whether they have the right composition and skill sets. The composition of the AC should be high performing members with the right skill sets and professional experience. It is also important that the committee have the bandwidth and members with the experience and skill sets necessary to oversee areas of risk beyond its core responsibilities that it has been assigned. For example, issues such as cyber and data security, AI and GenAI, ESG (including climate), or mission-critical risks such as safety, as well as supply chain issues and geopolitical risk, require more attention at the full board level Alternatively, a separate board committee or an additional sub-committee under the AC could take on the significant responsibilities related to cybersecurity and data governance.

Areas of focus

- AC should devote adequate time to understanding finances, GenAI, digital transformation, and climate/sustainability strategies. Additionally, it should help ensure that the finance function is attracting, developing, and retaining the leadership, talent, skill sets, and bench strength required to execute these strategies while continuing to fulfill its existing responsibilities. Staffing deficiencies in the finance department may pose the risk of a significant internal control breakdowns. Similarly, it is important for organisations to be alert to the risks associated with over-reliance on technology too quickly. Additionally, ACs should be mindful that CFO (and senior finance staff) succession is getting more difficult as individuals with the full breath of skills required are in short supply
- As the committee's workload expands to include oversight of disclosures of non-financial information it is important that ACs have the necessary financial reporting and internal control expertise to effectively carry out these responsibilities as well as its core oversight responsibilities. Further, it is important to assess whether the committee has the time, and the right composition and skill sets to oversee the major risks on its plate. Such an assessment is sometimes done in connection with a reassessment of issues assigned to each board standing committee.

Questions for the audit committee to consider

1. How does the organisation ensure that finance function attracts, develops, and retains the leadership, talent, skill sets, and bench strength needed to execute those strategies, while fulfilling its existing responsibilities?
2. Does the committee have the leadership, composition, skill sets and agenda time to carry out its core oversight responsibilities - financial reporting and internal controls along with the growing range and complexity of other risks, such as cyber and data security, supply chain issues and geopolitical risk, ESG risks and disclosures, or climate?
3. Is the committee relying only on one or two members to do the 'heavy lifting' in the oversight of financial reporting and controls?
4. Does the committee need to hire experts in order to discharge its oversight duties?

KPMG in India contact:

Ritesh Tiwari
Partner,
Board Leadership Center
E: riteshtiwari@kpmg.com

kpmg.com/in

kpmg.com/in/socialmedia

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000.