KPMG

MIoD
Mauritius Institute of Directors
Promoting Corporate Governance across the boach

Audit Committee Forum

Position Paper 13

Future-Ready Audit Committees: Technology & Talent Readiness



October 2026

kpmg.com/mu
miod.mu

About the Audit Committee Forum

Recognising the importance of Audit Committees as part of good Corporate Governance, the Mauritius Institute of Directors (MIoD), and KPMG in Mauritius have set up the Audit Committee Forum (the Forum) in order to help Audit Committees in Mauritius, from both the public and the private sectors, improve their effectiveness.

The purpose of the Forum is to help Audit Committee members adapt to their changing role. Historically, Audit Committees have largely been left on their own to keep pace with rapidly changing information related to governance, risk management, audit issues, accounting, financial reporting, current issues, future changes, and international developments.

The Forum provides guidance for Audit Committees based on the latest legislative and regulatory requirements. It also highlights best practice guidance to enable Audit Committee members to carry out their responsibilities effectively. To this end, it provides a valuable source of information to Audit Committee members, and acts as a resource to which they can turn for information or to share knowledge.

The Forum's primary objective is thus to communicate with Audit Committee members and enhance their awareness and ability to implement effective Audit Committee processes.

Position Paper series

The Position Papers, produced periodically by the Forum, aim to provide Board directors and specifically Audit Committee members with basic best practice guidance notes to assist in the running of an effective Audit Committee.

Position Paper 13 deals with Future-Ready Audit Committees: Technology & Talent Readiness.

*Previous Position Papers

- Paper 1: Best Practice Guidance Notes for Audit Committees (July 2014)
- Paper 2: Interaction of Audit Committee with Internal and External Auditors (May 2015)
- Paper 3: The Audit Committee's Role in Control and Management of Risk (December 2015)
- Paper 4: Guidelines for the Audit Committee's assessment and response to the Risk of Fraud (October 2016)
- Paper 5: Guidelines for the Audit Committee's approach to Information Technology risk (July 2017)
- Paper 6: Audit Committee Guidelines for evaluating a whistleblowing system (September 2018)
- Paper 7: Audit Committee's Guidelines for the Evaluation of Retirement Obligations (August 2019)
- Paper 8: Guidelines for the Audit Committee on Data Protection (October 2020)
- Paper 9: Guidelines for the Audit Committee on Business Continuity (October 2021)
- Paper 10 : Management of Cyber security risks in the new normal (October 2022)
- Special Edition on 10th Anniversary of ACF: 100 Best practices for Audit Committees (October 2023)
- Paper 11: Effective Audit Committee conversations (October 2024)
- Paper 12: Ethical considerations around data management (October 2025)

Previous Position Papers may be consulted/ downloaded from: KPMG Southern Africa and https://miod.mu/publications/position-papers/

Contents

1. Introduction 1
2. The Changing Risk Landscape 3
3. Technology Readiness: Enabling Trusted Reporting 5
4. Talent Readiness: A Strategic Oversight Priority 7
5. Strategic Implications for Organisations 9
6. Governance & Assurance Responsibilities 11
7. Practical Oversight Toolkit: Audit Committee Checklist 13
8. Conclusion 16

Members of the Forum

Collectively, the Forum is made up of the following members drawn from diverse professional backgrounds with significant experience in both the private and the public sectors.

Ujoodha Sheila – Chairperson	Langlois Stephane
Ah-Hen Clairette	Mahadea Sathan Anousha
Angoteea Ajay	Molaye Sanjay
Gooroochurn Bharatee	Mooroogen Sumita
Kee Mew Mervyn	Ong Su Lin
King Antoine	Puddoo Shashi
Koenig Fabrice	Ramdhonee Kalindee
Lan Desire	
Secretary: Bishundat Varsha	MIoD Coordinator: Mulung Nafeeza







01 Introduction

Audit Committees are operating in an environment that is fundamentally different from the one in which their traditional mandates were established. Rapid technological advancement, digital transformation, evolving cyber threats, and changing workforce dynamics are reshaping organisational risks and opportunities. While oversight of financial reporting and compliance remains important, Audit Committees are increasingly expected to provide broader oversight of technology-related risks, organisational resilience, and workforce capability. To remain effective, they must be equipped to oversee both technological transformation and talent readiness in an increasingly complex and digital business environment.

The global risk environment is undergoing rapid transformation driven by disruptive technology, increasing cyber vulnerabilities, and complex societal shifts. Research from the World Economic Forum (WEF), Institute of Risk Management (IRM), AXA, BDO, UMSA, and KPMG shows that organisations are entering a period of permanent risk turbulence, where traditional risk management approaches are no longer sufficient. The pace of digital transformation, the rise of automation and artificial intelligence (AI), and the escalation of cyber threats have converged to create a multidimensional and interdependent risk landscape.

This paper argues that leaders must evolve beyond compliance-focused risk processes towards integrated, technology-enabled, and human-centric resilience strategies. The analysis highlights four core areas shaping the modern enterprise:

1 The rising complexity created by digital transformation, automation/AI, and cyber threats.

2 The growing importance of data governance, including data quality, integrity, security, privacy, and the responsible use of information for decision-making.

3 The deepening interdependence between people (talent) and systems (technology).

4 The implications for organisational control environments, reporting integrity, and operational resilience.

In this context, Audit Committees must evolve from retrospective assurance providers into forward-looking oversight bodies. They are expected to anticipate emerging risks, challenge management on resilience and preparedness, and ensure that the organisation is equipped to operate effectively in a rapidly changing environment.

The conclusion is clear: resilient organisations will be those that build aligned ecosystems of skilled people, trusted technologies, and adaptive governance structures.

02



The Changing Risk Landscape

The modern risk landscape is defined by complexity, interconnectivity, and speed of change. Organisations are increasingly reliant on digital platforms and automated processes, which introduce both efficiencies and vulnerabilities.

Digital Transformation and System Dependency

Digital transformation continues to redefine business models, operational processes, and customer engagement. However, its speed and reach are introducing an unprecedented degree of complexity and uncertainty. According to the World Economic Forum's 2025 Global Risks Report, organisations are operating within an "increasingly fractured global landscape" in which digital systems evolve faster than governance mechanisms designed to regulate them. Similarly, the Institute of Risk Management (IRM) notes that organisations are struggling to adapt their risk frameworks quickly enough to keep up with the dynamically changing digital ecosystem. [kpmg.com] [scitechtimes.com].

This rapid transformation multiplies potential points of failure, increases reliance on interconnected platforms, and introduces new forms of strategic, operational, and ethical risk. Leaders must therefore focus not only on technological adoption but also the strengthening of governance and oversight structures to prevent the widening of internal risk gaps.

Automation and Artificial Intelligence

Artificial intelligence (AI) and automation are increasingly embedded in business operations and decision-making processes. While these technologies can enhance productivity and insight, they also introduce risks relating to transparency, accountability, bias, and control. The rapid adoption of AI has heightened concerns around data integrity, ethical use, and emerging threats such as deepfakes and shadow AI. Organisations must establish clear governance frameworks to ensure that AI is deployed responsibly and effectively.

Cybersecurity and Data Risk

As organisations become more digitally connected, cybersecurity and data governance have emerged as critical business priorities. Cyber threats continue to increase in scale and sophistication, with the potential to disrupt operations, damage reputation, and erode stakeholder trust. At the same time, organisations rely on vast volumes of data to support decision-making and innovation. Effective data governance is therefore essential to ensure data quality, integrity, privacy, security, and regulatory compliance. Building cyber resilience and maintaining trusted data environments are no longer purely technical concerns but strategic imperatives requiring board-level oversight.

Interdependence of People and Technology

Technology alone cannot deliver organisational resilience. Its effectiveness depends on the capabilities, judgement, and behaviours of the people who design, manage, and use it. However, many organisations face growing shortages of specialised skills in areas such as cybersecurity, data analytics, and AI. As digital transformation accelerates, leaders must invest in talent development, digital literacy, and a culture that promotes ethical and secure use of technology. Sustainable resilience is achieved when technology, people, and governance frameworks work together to support organisational objectives.

03

Technology Readiness: Enabling Trusted Reporting

Technology readiness is fundamental to reliable reporting, effective risk management, and organisational resilience. As organisations become increasingly dependent on digital systems, automation, artificial intelligence (AI), and data-driven decision-making, Audit Committees must ensure that the technology environment supports trusted reporting and effective governance.

System Integrity and Controls

Financial reporting processes are increasingly driven by automated systems and digital workflows. While automation can improve efficiency and reduce human error, weaknesses in system design, access controls, or change management can undermine the reliability of reporting. Audit Committees should seek assurance that critical systems are appropriately governed, monitored, and regularly tested.

Data Governance and Quality

Reliable reporting depends on accurate, complete, and consistent data. Poor data quality can compromise both financial and operational decision-making, regardless of the sophistication of the technology used. Organisations should establish clear data ownership, effective validation processes, and accountability for data integrity across key reporting systems.

Automation and AI Governance

The use of automation and artificial intelligence (AI) is expanding rapidly across finance, operations, and reporting functions. While these technologies can enhance efficiency, accuracy, and insight generation, they also introduce new risks that require effective governance and oversight.

Audit Committees should ensure that management understands and actively manages risks arising from both approved AI solutions and the growing use of publicly available AI tools by employees (shadow AI). Key areas of focus include:

- Accuracy and reliability of outputs: AI-generated information may appear credible but can be inaccurate, incomplete, or fabricated, creating risks for decision-making and reporting.
- Bias and fairness: AI models may replicate or amplify biases within underlying data, potentially resulting in unfair or discriminatory outcomes.
- Transparency and explainability: Organisations should be able to understand and explain how significant AI-driven decisions are generated.
- Data confidentiality and privacy: The use of external AI tools may expose sensitive organisational information if appropriate controls are not in place.
- Ongoing monitoring and governance: AI systems require continuous testing and monitoring to ensure they operate as intended and remain aligned with organisational objectives.
- Financial reporting implications: Where AI is used to support forecasting, analysis, or report preparation, outputs should be independently reviewed and challenged before being relied upon.

As AI adoption accelerates, organisations should establish clear governance frameworks, acceptable-use policies, and accountability structures to ensure that innovation is balanced with effective risk management and control.

AI Risks in Practice

AI-related risks are no longer theoretical. A number of high-profile incidents and illustrative scenarios below demonstrate how weaknesses in governance, oversight, and controls can result in financial, operational, regulatory, and reputational consequences. Audit Committees should be aware of the following key risk areas:

Risk Area	Illustrative Example	Key Consideration for Organisations
Incorrect or Fabricated Information	Air Canada's chatbot provided inaccurate information on bereavement fares, with the airline ultimately held responsible for the misinformation.	Organisations remain accountable for information generated by AI. Outputs influencing decisions, customers, contracts, or reporting should be appropriately reviewed and validated.
Bias and Discriminatory Outcomes	Recruitment software used by iTutorGroup allegedly excluded older applicants based on age and gender criteria.	AI models may inherit or amplify biases within data or design. Organisations should assess fairness, explainability, and compliance with legal and ethical requirements.
Inadequate Testing and Monitoring	Rite Aid's facial recognition system reportedly generated significant false-positive matches, raising concerns over governance and oversight.	AI systems require ongoing testing and monitoring throughout their lifecycle to identify inaccuracies, bias, and unintended consequences.
Deepfakes and Financial Fraud	A Hong Kong employee was deceived by AI-generated deepfake participants in a video meeting, leading to substantial fraudulent payments.	Traditional methods of verifying identity may no longer be sufficient. High-risk transactions should be independently validated through established approval channels.
Confidentiality and Shadow AI	Employees increasingly use public AI tools to analyse or generate content using organisational data.	Clear policies should define acceptable AI use, protect confidential information, and provide guidance on approved AI platforms.
AI in Financial Reporting	Organisations are increasingly using AI for forecasting, analysis, and report preparation.	Management remains responsible for the accuracy of financial information regardless of how it is produced. AI-generated outputs should be independently reviewed and challenged.

Cybersecurity and Third-Party Risk

As organisations become more interconnected, cyber threats and third-party dependencies continue to increase. Cyber incidents can disrupt operations, compromise sensitive information, and affect stakeholder confidence. Similarly, weaknesses in outsourced service providers or cloud platforms can expose organisations to significant operational and compliance risks. Effective oversight requires a clear understanding of cyber risks, supplier dependencies, and the controls in place to manage them.

Resilience and Business Continuity

Technology failures can have significant operational and financial consequences. Organisations should maintain robust disaster recovery and business continuity arrangements, supported by regular testing and review. The ability to recover critical systems and reporting processes quickly is an essential component of organisational resilience.

04

Talent Readiness: A Strategic Oversight Priority

Talent readiness is increasingly becoming a critical determinant of an organisation's ability to manage risk and maintain effective governance. The accelerating pace of digital transformation, AI adoption, cyber threats, and evolving business models is reshaping the capabilities organisations require to operate effective control environments. While many organisations have invested significantly in systems, technology, and governance frameworks, the skills required to oversee these evolving risks have not always developed at the same pace. As a result, Audit Committees should view talent readiness not merely as a workforce issue, but as a strategic risk and governance priority.

Current Position: Strong Foundations but Emerging Challenges

Most organisations have established strong foundations within traditional finance, audit, and compliance functions. Investments in learning and development programmes, digital transformation initiatives, and succession planning frameworks have helped support operational and governance objectives. In addition, increasing reliance on technology and digital processes has heightened the need for specialised skills across technology, data, risk, and assurance functions.

However, these initiatives are often developed independently rather than as part of an integrated talent strategy linked to the organisation's risk profile. As risks evolve, particularly in technology-driven environments, organisations are increasingly finding that existing capabilities may not be sufficient to provide effective oversight and challenge.

Broadening Expertise Beyond Traditional Functions

Strong finance and audit capabilities remain essential, but they are no longer sufficient on their own. Organisations increasingly require expertise in areas that were not traditionally considered core governance competencies. In particular, the ability to understand and challenge technology-related risks is becoming a critical requirement for both management and oversight functions.

Key capability areas include:

- Financial reporting and assurance
- Information technology and cybersecurity
- Data analytics and digital systems
- Artificial intelligence governance
- Technology risk and digital governance

Without adequate expertise across these domains, organisations may struggle to identify emerging risks, evaluate complex control environments, or provide effective oversight of technology-enabled processes.

Managing Capacity and Key Person Dependency

A significant challenge faced by many organisations is the concentration of critical knowledge within a small number of individuals. This is particularly common within specialised functions such as cybersecurity, enterprise systems, data management, and regulatory reporting. The loss or absence of key personnel can create operational disruption, weaken control effectiveness, and reduce management's ability to respond to emerging risks.

Audit Committees should therefore seek assurance that management is actively reducing key person dependency through:

- Cross-skilling and role rotation
- Knowledge transfer programmes
- Process documentation and standardisation
- Workforce planning for critical functions

Reducing dependency on individual expertise helps strengthen organisational resilience and improves continuity during periods of change or disruption.

Succession Planning and Continuous Upskilling

Succession planning remains an important element of talent readiness, particularly for leadership and specialist roles. While many organisations have documented succession plans, fewer have assessed whether identified successors are genuinely prepared to assume critical responsibilities. Effective succession planning requires regular review, targeted development, and periodic testing of readiness.

At the same time, rapidly evolving technologies are placing increased pressure on organisations to continuously update workforce capabilities. Traditional training approaches that rely on periodic interventions are often insufficient to keep pace with developments in automation, AI, cybersecurity, and digital transformation. Organisations should therefore establish a culture of continuous learning that enables employees to develop skills on an ongoing basis and respond effectively to changing risks and regulatory expectations.

Moving Forward: Aligning Talent with Risk

To strengthen resilience and governance effectiveness, organisations should ensure that talent strategies are directly aligned with their risk profiles. Capability requirements should be assessed in the context of key strategic and operational risks, with targeted investment in areas where capability gaps exist.

For Audit Committees, the key question is no longer whether the organisation has sufficient headcount, but whether it has the right capabilities to manage current and emerging risks. Organisations that invest in multidisciplinary skills, continuous capability development, and succession readiness will be better positioned to maintain effective governance and adapt to an increasingly complex risk landscape.




05
31%
84%
37% 67% 21% 44% 30% 89% 67% 29% 78% 68% 54% 57% 24% 65%
2020-2025
2015-2020
2010
-105.907
204.661
The World Economic Outlook (WEO) database contains selected macroeconomic data series from the statistical appendix of the World Economic Outlook report, which presents the IMF staff's analysis and projections of economic developments at the global level, in major country groups and in many individual countries. The WEO is released in April and September/October each year.
Use this database to find data on national accounts, inflation, unemployment rates, balance of payments, fiscal indicators, trade for countries and country groups (aggregates), and commodity prices whose data are reported by the IMF.
Data are available from 1980 to the present, and projections are given for the next two years. Additionally, medium-term projections are available for selected indicators. For some countries, data are incomplete or unavailable for certain years.
Due to the high level of uncertainty in current global economic conditions, the April 2020 WEO database and statistical tables contain only these indicators: real GDP growth, consumer price index, current account balance, unemployment, per capita GDP growth, and fiscal balance. Projections for these indicators are provided only through 2021.
The Timorese authorities have revised the compilation methodology of GDP and, under the new classification, oil and gas revenue before September 2019, which was previously classified as export in national accounts, is now classified as primary income.

Strategic Implications for Organisations

Evolving Control Environments

Control environments must move away from static, compliance-driven models toward more integrated and adaptive governance structures. A common challenge is that some organisations adopt a "box-ticking" approach to risk management, focusing on compliance activities rather than addressing underlying vulnerabilities.

Control environments can evolve by embedding technology, continuous monitoring, and data-driven controls into governance processes. Organisations should also invest in change management, workforce upskilling, and a culture of accountability to strengthen talent readiness. This creates a flexible, risk-based control environment that supports innovation while maintaining effective governance and resilience.

KPMG's insights indicate that the expansion of AI and cyber-related risks requires leaders to integrate governance frameworks that reflect evolving technological realities. This includes establishing clear oversight roles, strengthening system controls, and promoting cross-functional collaboration.

Strengthening the Reliability of Reporting

As digital systems automate and accelerate reporting, outdated systems, insufficient data governance and opaque AI-driven outputs can create gaps in visibility and undermine the reliability of information. Organisations therefore need to ensure that their data infrastructure keeps pace with changes in reporting processes.

Evolving requirements around data protection, AI governance, cyber resilience and digital compliance add to this complexity. Accurate data, transparency and ethical governance remain essential, particularly where AI is used in reporting and decision-making.

Operational Resilience as a Strategic Imperative

Operational resilience is no longer only about recovering from disruptions; it is about developing an organisation capable of absorbing shocks and emerging stronger. Organisations must prioritise flexibility, innovation and proactive scenario planning to strengthen operational resilience and respond effectively to emerging risks. "KPMG's analysis highlights the growing focus on cyber resilience and operational resilience, with regulatory developments such as the Digital Operational Resilience Act (DORA) reinforcing expectations around ICT risk management, cybersecurity governance, and resilience." [kpmg.com]

War for talent

An organisation's ability to implement technology successfully depends as much on people as on systems. An effective control environment must therefore evolve beyond traditional controls to include talent attraction, retention, continuous learning, succession planning, and change management. Organisations that successfully align technology readiness with talent readiness will be better positioned to maintain strong governance, effective internal controls, and sustainable long-term performance.

Change management

An effective control environment evolves by integrating change management into governance, culture, and internal controls. Successful digital transformation depends not only on implementing new technologies but also on preparing people to embrace and sustain change. Through strong leadership, continuous communication, employee engagement, ongoing training, and effective monitoring, organisations can build a resilient control environment that supports innovation while maintaining sound governance and risk management.

06


Oct 19
Nov 19
Dec 19
Jan 20
Feb 20
Mar 20
Apr 20
Jun 20
Jul 20
Aug 20
Sep 20
Income
09.03.19
Sales:
21.39%
04.55%
23.98%
65.98%
Making Department
Film Departmeent
Post Department
Q3
Operating Cost:
Making Department
Film Departmeent
Post Department
Compare
Jul 2019
48181 p.
78181 p.
03174 p.
31411p.
65135 p.
03154 p.
Refresh

Governance & Assurance Responsibilities

Effective oversight of technology and talent readiness depends on a strong governance framework supported by capable management, Internal Audit, and an informed Audit Committee. As organisations become more reliant on digital systems, data, AI, and specialised skills, the traditional boundaries between financial oversight, operational risk, and technology governance are increasingly blurred.

Management Accountability

Management remains responsible for designing, implementing, and maintaining effective systems, controls, and organisational capabilities. This includes ensuring that technology environments are secure and resilient, while also developing the skills required to operate and oversee these environments effectively.

A common challenge is the imbalance between investments in technology and investments in people. Organisations may implement sophisticated systems without building the capabilities needed to govern them effectively, creating risks that can undermine the expected benefits of transformation initiatives.

The Evolving Role of Internal Audit

Internal Audit plays a critical role in providing independent assurance over technology, talent, and governance risks. To remain effective, Internal Audit must become increasingly agile, technology-enabled, and forward-looking.

Key areas of focus should include:

- Technology and cybersecurity risks
- Data governance and data quality
- AI governance and automated controls
- Third-party technology dependencies
- Talent readiness and key-person risks
- Organisational resilience and business continuity

Rather than validating every individual transaction or data point, Internal Audit should assess whether the underlying systems, controls, and governance processes are capable of producing reliable and accurate information.

Internal Audit also has an important role in providing assurance over the use of AI. As organisations increasingly adopt AI-enabled tools for analysis, forecasting, and reporting, auditors should evaluate whether appropriate governance, validation, monitoring, and oversight mechanisms are in place. AI can improve efficiency, but it should complement, not replace, professional judgement.

Audit Committee Oversight

The Audit Committee plays a pivotal role in ensuring that technology, talent, and assurance functions operate cohesively. Its responsibility extends beyond reviewing reports to actively challenging management and ensuring that emerging risks are understood and appropriately managed.

To fulfil this role effectively, Audit Committees should focus on:

- Whether technology and talent strategies are aligned with the organisation's risk profile.
- The adequacy of Internal Audit's coverage of emerging risks.
- The effectiveness of cybersecurity, data governance, and AI oversight frameworks.
- Key-person dependencies and succession readiness for critical roles.
- The resilience of critical systems and business processes.
- Management's preparedness for future technology and workforce challenges.

07

Practical Oversight Toolkit: Audit Committee Checklist

To strengthen oversight of technology and talent readiness, Audit Committees should adopt a disciplined approach to inquiry. The following questions are designed to support meaningful engagement with management and the Board, enabling deeper insight into the organisation's preparedness, resilience, and risk posture.

A few questions to be considered by Audit Committee members include:

Data Governance & Technology Readiness

A. Data Governance and Data Quality

- Who is accountable for the quality and integrity of key data used in financial and operational reporting?
- How do we ensure that data is accurate, consistent, and complete across systems?
- What processes are in place to identify and remediate data quality issues?
- How are we ensuring compliance with the Mauritius Data Protection Act and related data privacy requirements?
- To what extent do we rely on data for decision-making, and how confident are we in the accuracy and reliability of that data?
- How do we ensure that data used to train, operate, or support AI-enabled tools is accurate, reliable, and appropriately governed?

B. Technology Environment and System Resilience

- Are our core systems stable, secure, and scalable to meet future business requirements?
- How are system upgrades, patches, and changes governed and controlled?
- What are the most critical system dependencies, and how are these risks managed?
- How quickly can we recover from a major system failure, and when was this last tested?
- Are our current technology investments aligned with our long-term strategic objectives?

C. Cybersecurity and Incident Preparedness

- What are the most significant cyber risks currently facing the organisation?
- How do we monitor and respond to emerging cyber threats?
- When was the last independent cybersecurity assessment conducted, and what were the key findings?
- How prepared are we to respond to a cyber incident, and have response plans been tested through simulations?
- What level of cyber awareness exists across the organisation, including senior management and staff?

D. Third-Party and Outsourcing Risk

- Which critical systems or processes are dependent on third-party providers?
- How do we assess and monitor the risks associated with these providers?
- What contractual safeguards are in place regarding data protection, service continuity, and incident response?
- Do we have sufficient visibility over subcontracting arrangements used by our vendors?
- What contingency plans exist in the event of a failure of a key service provider?

E. Business Continuity and Operational Resilience

- Do we have a comprehensive and up-to-date business continuity plan?
- How frequently are disaster recovery and continuity plans tested, and what were the outcomes of the most recent tests?
- What are our recovery time objectives for critical systems, and are these realistic?
- How prepared are we for Mauritius-specific risks such as cyclones, infrastructure disruptions, or connectivity issues?
- Can we maintain critical operations during prolonged disruptions?

Talent Readiness

F. Talent Capability and Skills Readiness

- Do we have sufficient in-house expertise in key areas such as IT, cybersecurity, and data analytics?
- Where are we most reliant on a small number of individuals, and how are these risks being managed?
- What are the most critical capability gaps in the organisation today?
- How are we addressing challenges in attracting and retaining skilled talent in a competitive market?
- To what extent are we dependent on external consultants or service providers for critical capabilities?

G. Succession Planning and Leadership Continuity

- Do we have robust succession plans for key roles, including finance, IT, and internal audit leadership?
- How frequently are these plans reviewed and updated?
- How would the organisation respond to the unexpected departure of a key individual?
- Are we developing internal talent pipelines to reduce reliance on external hiring?

H. Alignment of Talent and Technology

- Are our talent capabilities aligned with our current and future technology landscape?
- Do we have the necessary skills to effectively manage and oversee the systems we are investing in?
- Are we implementing new technologies faster than we can build internal capability to support them?
- How well are IT, finance, risk, and HR functions coordinated in managing these interdependencies?
- What risks arise from any misalignment between our people and our systems?

Financial Reporting and Assurance

I. Financial Reporting and Systems Integrity

- To what extent is our financial reporting dependent on automated systems, and where do manual interventions still exist?
- How do we ensure the integrity and completeness of data flowing across systems used for financial reporting?
- What controls are in place to prevent and detect unauthorised changes or overrides within financial systems?
- Have there been any recent system issues or control failures that could have impacted financial reporting accuracy?
- How confident are we that our current systems can support increasing reporting complexity and regulatory expectations?

J. Internal Audit and Assurance Effectiveness

- Does Internal Audit have the necessary expertise to assess technology and cyber risks effectively?
- To what extent does the Internal Audit plan cover IT systems, data governance, and cybersecurity?
- Are findings from technology-related audits being addressed promptly and effectively by management?
- Should we consider co-sourcing or external specialists to enhance assurance capabilities?

K. Audit Committee Effectiveness

- Do we, as an Audit Committee, have sufficient understanding of technology-related risks to provide effective oversight?
- Are we asking sufficiently probing and forward-looking questions?
- Do we receive clear, relevant, and timely information to support our decision-making?
- Should we seek additional training or external expertise to strengthen our effectiveness?



08 Conclusion

Audit Committees are operating in a fundamentally different environment from the one in which their traditional roles were defined. Rapid digital transformation, increasing reliance on complex systems, and evolving risk landscapes mean that oversight can no longer be limited to historical financial reporting. Instead, Audit Committees must adopt a more forward-looking and strategic approach, focused on resilience, preparedness, and emerging risks.

Central to this shift is the alignment between **technology and talent**. Reliable financial reporting, effective risk management, and operational continuity now depend on both robust systems and the capability of the people who manage them. Weakness or misalignment in either area can expose organisations to significant risk, making integrated oversight essential.

In Mauritius, this challenge is amplified by increasing digital adoption, reliance on third-party providers, and constraints in specialised talent. Audit Committees must therefore play a more active role in ensuring that organisations are not only investing in technology, but also building the skills and structures needed to support it.

Ultimately, future-ready Audit Committees will be those that move beyond compliance-driven oversight to provide informed challenge and strategic direction. By strengthening the alignment between technology and talent, they can enhance governance, support resilience, and help sustain long-term value in an increasingly complex environment.

"Every digital transformation begins and ends with people."
— Satya Nadella

References

https://nexttechtoday.com/tech/cyber-security/is-your-cybersecurity-ready-for-ai-in-2025/

https://www.weforum.org/publications/global-risks-report-2025

[assets.kpmg.com], [kpmg.com]
Moffatt v. Air Canada, 2024 BCCRT 149 (B.C. Civil Resolution Tribunal, 14 Feb 2024).

https://www.canlii.org/en/bc/bccrt/doc/2024/2024bccrt149/2024bccrt149.html

U.S. EEOC, press release, 11 Sep 2023; EEOC v. iTutorGroup, Inc., No. 1:22-cv-02565 (E.D.N.Y.).

https://www.eeoc.gov/newsroom/itutorgroup-pay-365000-settle-eeoc-discriminatory-hiring-suit

U.S. FTC, press release, 19 Dec 2023, FTC v. Rite Aid Corp. (E.D. Pa.).

https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without-reasonable-safeguards

South China Morning Post, "UK multinational Arup confirmed as victim of HK$200 million deepfake scam, " May 2024.

https://scmp.com/news/hong-kong/law-and-crime/article/3263151/uk-multinational-arup-confirmed-victim-hk200-million-deepfake-scam-used-digital-version-cfo-dupe

KPMG
KPMG Centre
31 Cybercity, Ebène, Mauritius
T: (230) 406 9999 **F:** (230) 406 9998
E: kpmg@kpmg.mu **W:** KPMG.com/mu
Business registration number: F07000189

Mauritius Institute of Directors
6th Floor, Building A5, Hyvec Business Park
15 Wall Street, Ebene 72201, Mauritius
T: (230) 468 1015 **F:** (230) 468 1017
E: info@miod.mu **W:** miod.mu
Business registration number: C08077130

kpmg.com/socialmedia

Disclaimer:

The information contained in Position Papers disseminated by the Audit Committee Forum is of a general nature, and is not intended to address the circumstances of any particular individual or entity. The views and opinions of the Forum do not necessarily represent the views and opinions of KPMG, the Mauritius Institute of Directors and/or individual members. These guidelines are for discussion purposes only and in considering the issues, the culture of each entity should be taken into account as must the charter for each entity's Audit Committee. Although every endeavour is made 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 reliance should be placed on these guidelines, nor should any action be taken without first obtaining appropriate professional advice. The Audit Committee Forum shall not be liable for any loss or damage, whether direct, indirect, consequential or otherwise which may be suffered, arising from any cause in connection with anything done or not done pursuant to the information presented herein.

This publication does not provide guidance on how to deal with individual situations, nor does it provide a complete description of relevant legislation. Reference may need to be made to the legislation and other pronouncements mentioned in the text and to the organisation's professional advisers for detailed information.