Accelerate

Perspective on the key issues driving the Audit Committee agenda

2018 Edition

kpmg.ca/accelerate

Contents

Introduction

By **Kristy Carscallen**
Canadian Managing Partner, Audit
KPMG in Canada

Audit committees are no strangers to change. The days ahead promise constant technological change and with that newfound risks. Today's scale of disruption is rewriting the audit committee's agenda in unprecedented ways, and it's a transformation that demands attention across the board.

In this inaugural *Accelerate* report, we identify seven of the key trends impacting organizations today that are disrupting the audit committee mandate – blockchain, cyber threats, internal controls, data management and security, finance function automation, risk, and expanded forms of external reporting.

Whether adapting new technologies or adopting fresh risk management strategies (e.g., data management, cyber security, internal controls, etc.), it's no exaggeration to say that audit committee members and management now have more on their plate than ever before.

Transformation can be intimidating – especially on today's scale. Nevertheless, these mounting expectations and responsibilities can be overcome by embracing disruption, learning the risks and rewards of new technologies, and resisting the urge to stay static.

Organizations are trying to accelerate growth all the while dealing with disruption, risk, cyber threats, and other strategic issues. Audit committees have always been adept at adapting to their organization's needs, and now is no different.

In the pages that follow, subject matter leaders from across KPMG in Canada examine current trends and spotlight the many opportunities and challenges in the audit committee's path. We hope the information and insights in this report will help you successfully respond to these issues and provide confidence in your organization's ability to embrace the change to come.

Prepare for the blockchain revolution

By **Paritosh Gambhir**
Head of Blockchain, GTA Audit Innovation Leader
Partner, Audit Financial Services
KPMG in Canada

Additional insights

Still waiting for the blockchain fad to fade? You may want to take a seat. Digital ledgers and peer-to-peer networks are fast becoming the "new normal" among future-facing companies and reshaping how the world transacts.

It's a technological rush that's catching everyone in its wake. That includes audit committee members who share a responsibility for learning the latest in blockchain technologies and ensuring their organizations are thinking about which processes may be ripe for blockchain transformation (e.g., know your customer (KYC), derivatives or securities trading, supply chain management, customer experience, etc.). Audit committees need to understand the risks that come with blockchain and determine what internal controls management has in place to ensure that every link along the chain is performing as expected. Following the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework can help in these critical stages, as can working with blockchain consultants who have travelled the implementation path and know what to expect.

And implementation is only the beginning. The next – and arguably most critical step – is governance over the blockchain. Does management have clear guidelines on who can be added to the chain? What protocols will the organization employ? How will activity be monitored and who will ultimately take responsibility for the chain at the end of the day? Given the nature of blockchain, the information (with the value associated) recorded is practically immutable, it must be made clear how information (and value embedded within) is added, who has control and access, and when (or even if) compliance checks are occurring.

It's paramount that the audit committee gets the governance aspect of blockchain right – especially from an internal controls perspective. As organizations adopt blockchain, the costly compliance, reporting, and internal control requirements that are typically associated with SOX will likely decrease. This is especially true if the intent is to integrate blockchain into an existing financial or risk system or another legacy process. Here again, knowing and understanding the technology, understanding the risks, and establishing organization-wide controls is essential.

Ready or not, blockchain technologies are here to stay. As organizations look to digital ledgers and decentralized networks to optimize an increasing number of tasks, the onus is on audit committees to ensure the risks that go along with the emerging technology are adequately managed.

What should Audit Committees be asking?

– Does management have a blockchain strategy?

– Does management have a well-established control environment and framework?

– What internal controls are in place to protect your organization against risks associated with emerging technologies such as blockchain?

– What problems or issues does the blockchain strategy address?

Cyber: An Audit Committee imperative

By **Hartaj Nijjar**
Partner, Cyber Security
KPMG in Canada

Additional insights

Cyber security is no longer just an IT problem – it's a significant business risk. In the age of disruption and mounting online risks, digital security is a responsibility all departments must bear. That includes audit committees who need to become more flexible in their approach, dynamic in their execution, and in-tune with today's cyber risk environment.

Audit committees aren't the only line of defense, but they are critical nonetheless. With IT and information security professionals on the frontlines, it falls to audit committee members to support their efforts by building awareness around threats to their financial functions, promoting best practices, and making sure their organization is taking appropriate actions to shore its cyber defenses.

Serving that role means asking the fundamental questions: How effective is our organization's cyber strategy at identifying and addressing cyber risks? Is it relying on the right information to oversee and understand those risks? Is it addressing all of its data privacy and security obligations? Does it have a game plan in place to manage a cyber crisis when an incident occurs?

Third party risk must also be part of the conversation. Organizations are extending their digital footprints via cloud, blockchain, and other networked technologies and becoming more vulnerable to third-party risks as a result. Again, audit committees would do well to ask how the organization is tracking the use and security of its sensitive data among its external partners and how it is evaluating the integrity of the tools and software they themselves use.

The pace of change demands a nimble approach. Audit committees must evolve beyond their traditional approach to address disruptive technologies and cyber risk in real time. And while there may be knowledge and skill gaps around the topic of cyber, now is the time to collaborate with industry peers and consultants to build internal capabilities. Only then will audit committees fulfill their much-needed role in an organization's cyber posture.

What should Audit Committees be asking?

- How effective is my organization's cyber risk strategy? Is it focused on the right areas? Is it being tested?
- How does my organization's cyber posture compare to others in the industry? Where are its gaps?
- When a cyber incident occurs, how will it respond? How will it recover?

Internal controls are moving beyond SOX

By **Genevieve Leong**
Partner, Risk Consulting
KPMG in Canada

Additional insights

It's a coming of age for internal controls. Programs once designed to stay compliant with financial reporting laws are now maturing to protect organizations from critical enterprise risks. Many organizations have also evolved "how" they assess internal controls over financial reporting as well. It's a stark evolution from the early days of Sarbanes-Oxley (SOX) and a shift that's changing the landscape for audit committees.

Until recent years, organizations have approached "internal controls" from a SOX compliance perspective; that is, dedicating a lion's share of their focus on controls over financial reporting. This stemmed from the introduction of new and expanded financial reporting requirements in 2002 following a number of public corporate scandals.

Now, 15 years later, organizations are seeking to extract more value from their internal controls programs by streamlining effort and adopting new technological efficiencies. Some have expanded their internal control programs beyond financial reporting risks and re-examined internal controls through an enterprise and operational risk lens.

In short, the focus is evolving; and the resulting challenges (and opportunities) are requiring audit committees to consider technologies, reporting processes, and risks beyond their conventional financial scope. As advancements in robotic process automation, artificial intelligence, and data analytics continue to re-shape control environments, audit committees are becoming fluent in the new tools of their trade.

As organizational silos give way to centralized structures, they are increasing their awareness around internal controls related to all manner of risks, from cyber to fraud and beyond.

Cost-saving pressures are also influencing audit committees' approaches to internal controls. More and more organizations are leaning on all departments to extract greater value from their SOX programs. As such, audit committees are among those being asked to streamline their approach while maintaining the integrity – and budget – of the organization.

All told, it's a new day for internal controls. And as organizations embrace new approaches to traditional programs, it falls on audit committees to become familiar with their new landscape and move beyond their SOX foundations.

What should Audit Committees be asking?

- How has the organization evolved its internal controls program – from risk assessment, approach to evaluating the effectiveness of internal controls and reporting?
- What technologies is it embedding to reach that objective?
- How will these changes impact the audit committee's role, responsibilities, and processes?

Data management and security: Preparing for the inevitable

By **Corey Fotheringham**
Partner, National Leader Strategy & Operations
Forensic Technology and CyberCrime
KPMG in Canada

Additional insights

It's a familiar saying but one worth repeating: It's not a matter of *if* a cyber incident occurs but *when*. Many organizations are taking this modern adage to heart and making data security a priority across all functions – audit committees included.

The days of physical files and locked cabinets are fading. Today's audit committees work with sensitive financial data that must be stored, archived and shared via networks of servers, internal networks, and cloud-based services. And while there are endless advantages to going digital, the risks of having that data stolen, lost, or leaked are enough to make any audit committee member lose sleep.

After all, failure to protect financial data can trigger both financial and reputational damages. There are data regulations, mandatory reporting laws, and international privacy obligations (EU's GDPR) that carry significant penalties if not upheld. Moreover, becoming a public victim of a cyber attack can do irreparable damage to even the most reputable brands.

Audit committees don't necessarily bear the full weight of these risks. They do, however, play a critical role in upholding data management and security measures; as well as ensuring cyber security remains top-of-mind for their organizations' leaders. As custodians of vital client and organizational data, they need to ask the important questions:

What data are we managing? What value does it hold? Where is it being stored? If it was exposed, what would that mean for the company and how would we respond?

Like every other entity in an organization, audit committees share a responsibility for understanding their exposure, bringing attention to cyber security risks, and collaborating with colleagues to improve their strategies around data management and security. Only when all parties are working towards a stronger cyber posture can an organization be truly prepared for when a cyber disaster strikes.

What should Audit Committees be asking?

- What data do we manage? What value does it hold?
- If our data was stolen, what would be our exposure and how would the organization respond?
- What can we, the audit committee, do to bolster the organization's cyber posture?

Automation is changing the finance function

By **Stephanie Terrill**
Partner, Global Lead Financial Management
KPMG in Canada

Additional insights

Extreme automation is rapidly changing the very nature of how businesses and their finance functions operate. And as organizations move towards cloud-based services and data-driven systems, it's important that all parties embrace the automation of financial processes and controls through disruptive technologies like Cloud ERPs, artificial intelligence, cognitive computing, robotic process automation, and blockchain.

Extreme automation extracts risk from routine processes and provides the end user with more guaranteed process outcomes at a lower cost. It is most often applied to routine transaction processes and uses embedded application controls, exemption reporting, and cyber security controls testing to maintain integrity.

As the pressure for organizations to embrace new technologies and lower finance costs increases, the race to extreme automation accelerates. So too does the need for better awareness around how automation technologies work, connect to other functions, and alter the control environment. For audit committees, that due diligence includes asking management the right questions around the segregation of duties within and across key applications, and ensuring the CIO and head of internal audit are collaborating to address security and segregation of duties. The importance of establishing proper segregation of duties has existed long before disruptive technologies and extreme automation, but the task now is to apply the foundational principles of a control framework to a cloud and on-premises environment.

Third-party risk also warrants attention. As organizations take to Software as a Service (SaaS) en masse, they are welcoming more external parties into their digital network. That includes parties who may have designed and established their cloud-based service and external partners who have access to it on an ongoing basis. Here again, the access and segregation of duties are critical, both in terms of determining who has permission to remain in the system and in verifying their activity. It also pays to develop an understanding of third-party policies and roles, and build third-party risks into each individual contract.

Preparing for automation boils down to upholding one's duty of care. For audit committees, it also requires forging ahead with a sense of curiosity for new technologies, being open to extreme automation, and making peace with disruption.

What should Audit Committees be asking?

- Does management have the proper segregation of duties for automated systems?
- What oversight and policies do we have around Saas?
- How is management adjusting their risk and controls framework to address security as we bring in new automation technologies and software vendors?
- How is third-party risk being managed? Who are we doing business with and what due diligence was done on our alliance and vendors?

Risk belongs on every agenda

By **Heather Cheeseman**
Partner, Energy and Natural Resources
KPMG in Canada

Additional insights

Risk is subjective by nature. Threats and vulnerabilities differ from one organization to the next; as do the strategies and responsibilities for managing them. An Audit Committee's role will vary for this reason, yet it is most effective when supported by a robust board-level approach.

What does that robust board-level approach look like? It's the entire Board understanding its responsibility to oversee risk management. It's clearly defining roles and committee mandates to leverage the expertise of individual directors and committees so that collectively they ensure the organization has effectively identified, measured and prioritized its top risks. It's the Board assessing risk when committing to the organization's strategic plans, agreeing on and collectively monitoring the response.

We must remember that risk doesn't necessarily mean "threat". Risks can signal an opportunity for growth or innovation which an organization may choose to exploit. Strategic responses (to either mitigate the downside or take advantage of the upside) need to be informed by reliable information regarding the related risks and the organization's agreed appetite for risk.

Risks are never static. Neither can they be contained in silos. Risks evolve, expand, and connect to other risks in complex and unpredictable ways. Without a crystal ball, accurately predicting the impact of compounding and interconnected risks is impossible. But Boards must challenge management to comprehensively assess the dependencies between risks. Given the pace of change and complexities of doing business in an increasingly connected world, it's nearly impossible to fully understand and address every risk on the (virtual) horizon. Boards must remain focused on what threatens the achievement of the company's strategic objectives. Organizations need to prioritize risks based on their severity and likelihood, using an agreed framework or ranking scale.

The good news is, boards don't need to go it alone. There are numerous resources and third-party supports that can work with the board to bridge skill gaps and provide the tools and resources to pursue a truly dynamic risk management approach.

What should Audit Committees be asking?

- Are the roles and responsibilities for risk oversight clearly defined at the Board level?
- How is the organization identifying, measuring, and mitigating its critical risks?
- How have we considered the assessment of risk in determining the organization's strategic plan?
- How much risk is the organization willing to take to achieve its objectives?
- How have we assessed the impact of these risks in relation to each other? How dependent is one on the other or how will the outcome of one compound the severity of another?

External reporting: Moving beyond the status quo

By **Bill Murphy**
National Leader, Climate Change & Sustainability Services
KPMG in Canada

Additional insights

It's time to expand your oversight of external reporting. New trends and reporting directives are placing added expectations on audit committees. These need to be considered before various external reports are shared with outside stakeholders.

Within the annual report itself, securities regulators are placing significant attention on the use of non-GAAP measures in the management's discussion and analysis (MD&A) section and related press releases. In turn, audit committees are being encouraged to increase their focus on these measures and gain more comfort around the definition, use and reconciliation of these non-GAAP measures.

Attention also needs to be paid to new annual report content. This added content is being driven by multiple trends, the first being the emergence of frameworks such as the Task Force on Climate-related Financial Disclosures (TCFD) recommendations. These recommendations call for expanded disclosure of any material financial risks that climate change presents to the company's business model, services, supply chain, and customer base. Such risks could adversely affect access to capital and profitability. While currently voluntary, the recommendations are being studied by regulators including the Canadian Securities Administrators. Additional report content is also being driven by diversity reporting requirements.

The second trend is toward increased discussion of strategy and long term value creation. An example is the UK's Strategic Report requirements and related guidance from the Financial Reporting Council. Although a similar requirement does not yet exist for North American companies, major institutional investors are increasingly demanding expanded disclosures on how reporting issuers are positioned to create and sustain long term value.

There are a growing number of external communications beyond the annual report. These include sustainability and climate change reports, carbon disclosures, and a multitude of responses to investor surveys and questionnaires. There has been a corresponding emergence of an 'alphabet soup' of reporting frameworks, which create challenges to implement and oversee. To that end, a 'Corporate Reporting Dialogue' initiative among standard setters has been established to better align these frameworks.

Navigating these new forms of reporting requires reporting processes and controls beyond the traditional finance domain, and applying additional executive and audit committee oversight. Audit committees are encouraged to revisit the 'status quo' and inquire how this expanded information is being sourced, compiled, and published; and if their current disclosure controls and procedures are aligned with these new expectations.

What should Audit Committees be asking?

- Is your Committee mandate and the organization's disclosure controls and procedures sufficiently broad to address these expanded forms of reporting?
- How are expanded disclosures sourced, compiled, and published?
- How can the audit committee best stay abreast of these rapidly expanding forms of external reporting?

Let's do this.

As an Audit Committee member, you're responsible for helping to guide your organization through a range of issues and challenges that are broader and more complex than ever before. You need to focus on growth, risk and disruption, while still fulfilling your traditional governance and reporting mandate. For audit committees, this is the new normal.

While the challenge has never been greater, KPMG can help provide the confidence you need to navigate the changing audit and assurance landscape and empower you to accelerate your business growth. **Let's do this.**

Visit kpmg.ca/accelerate for video interviews of each of the subject matter leaders featured in this report.

Contributors

Kristy Carscallen
Canadian Managing Partner, Audit
KPMG in Canada
416-777-8677
kcarscallen@kpmg.ca
Connect on LinkedIn

Heather Cheeseman
Partner, Energy and Natural Resources
KPMG in Canada
416-777-3314
hcheeseman@kpmg.ca
Connect on LinkedIn

Corey Fotheringham
Partner, National Leader Strategy & Operations
Forensic Technology and CyberCrime, KPMG in Canada
416-218-7974
coreyfotheringham@kpmg.ca
Connect on LinkedIn

Paritosh Gambhir
Head of Blockchain, GTA Audit Innovation Leader
Partner, Audit Financial Services, KPMG in Canada
416-777-3335
pgambhir@kpmg.ca
Connect on LinkedIn

Genevieve Leong
Partner, Risk Consulting
KPMG in Canada
416-777-3226
genevieveleong@kpmg.ca
Connect on LinkedIn

Bill Murphy
National Leader, Climate Change &
Sustainability Services, KPMG in Canada
416-777-3040
billmurphy@kpmg.ca
Connect on LinkedIn

Hartaj Nijjar
Partner, Cyber Security
KPMG in Canada
416-228-7007
hnijjar@kpmg.ca
Connect on LinkedIn

Stephanie Terrill
Partner, Global Lead, Financial Management
KPMG in Canada
403-691-8374
sterrill@kpmg.ca
Connect on LinkedIn

kpmg.ca/accelerate