KPMG

Institute of Corporate Directors
Institut des administrateurs de sociétés

Audit Trends 2016

From transformative technology to complex regulation to unprecedented geopolitical risk, an increasing tide of disruptive trends are demanding substantive change to the global role of audit committees.

kpmg.ca/audit

Foreword

Challenging times demand challenging thinking

For audit committees, times have never been more challenging. Cyber security and technological disruption in general; economic volatility, particularly in the oil and gas sector; expanding global political and regulatory risk: a lengthening slate of risk issues is impacting today's corporate boards, with risk oversight, financial and otherwise, increasingly filtering down to the audit committee.

Kristy Carscallen
Canadian Managing Partner, Audit
KPMG in Canada

Stan Magidson
President and CEO
Institute of Corporate Directors

With this unprecedented wave of change leaving organizations in a seemingly perpetual state of transition, audit committees are dealing with a mandate that is constantly in flux, demanding more attention, more time and more thought than ever before. How do audit committees effectively oversee risk in this kind of environment?

Clearly, there's no one answer to that question. In *Audit Trends 2016: Targeting transformation*, disruption on multiple fronts is putting audit committees on high alert. We maintain that the path to clarity lies in asking the right questions—the challenging questions that today's audit and risk landscape demands—and framing them in terms that are provocative of thought, but also evocative of solutions. For example, the report begins by looking at key risks associated with technological disruption, from a range of cyber security exposures, to the dangers of competitive innovation undermining your business model, to the possibility of data & analytics (D&A) activities unintentionally exposing client data in unsanctioned ways.

Continuing the theme of disruption, the report outlines the ways economic volatility, emerging market risk, and geopolitics are driving a range of political and economic risks, potentially affecting the ways companies formulate financial strategy and suggesting the need to re-evaluate operations in particularly risky global jurisdictions.

This report then considers key global reporting trends, including integrated and strategic reporting, expanded audit reporting and enhanced operating and performance disclosures. Finally, there is an examination of mounting regulatory complexity that covers new and changing regulations and standards, their impact on Canadian audit committees and how this shifting environment is affecting audit committees' understanding of what constitutes audit quality.

The aspiration behind the report is to get people thinking differently and to consider how the audit committee mandate may need to change or expand. While the audit committee must of course remain steadfastly independent of management, it can still enhance its historical role by asking the tough, necessary questions and ensuring the extent of its oversight expectations are fully understood. Indeed, the Institute of Corporate Directors (ICD) has expanded its activities in this area, working closely with CPA Canada and CPAB (Canadian Public Accountability Board) on clarifying a number of audit committee matters—for example, submitting input from the director community on whether the benefits of Europe's current enhanced auditor reporting initiative would outweigh its costs if implemented in Canada.

That kind of stakeholder cooperation is an important step as audit committees strive to define and fulfill their responsibilities. It is our hope that this report will help audit committees and boards better navigate the difficult and evolving audit and risk environment.

© 2016 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Director commentary

Targeting transformation

Social engineering

"In addition to ensuring proper use policies are in place, it's important to constantly remind employees of the ongoing risk of social engineering and the types of attacks they may be subject to. A culture of consistent vigilance is crucial. HR needs to specifically tell people to protect passwords, ignore emails from people they don't know and avoid opening files they don't recognize. Audit committees, in overseeing social engineering risks, should be asking what those risks are, then inquiring into the existence of codes of conduct, the types of relevant training employees receive and what tactics they should be using to combat the issue."

John Clappison, Director

Regulatory complexity

"The impact of financial regulation—whether it deals with securities, financial institutions or auditors—is, and will continue to be, significant. But audit committees ignore the potential impacts of issuances from other regulatory entities at their own risk. Anyone in the pipeline, telecommunications, television or taxi businesses, for example, can tell you that regulations are increasing across the board. And oversight of compliance risk—regardless of which regulatory body it stems from—often falls to the audit committee."

Paul Weiss, Director

© 2016 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Contents

Audit Trends

© 2016 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Director commentary

Targeting transformation

Cyber risk

"The whole cyber risk and cyber security issue is certainly becoming a board responsibility to attract related expertise. The challenge arises, however, when too much of this mandate is shifted into the audit committee, where it isn't always appropriate and where the required acumen is less likely to be present. There has to be clarity on what an audit committee delivers. Issues such as disruption, cyber and D&A may not fit within an established committee, in which case the board may want to form appropriate, dedicated technology sub-committee or a technology advisory board."

Deborah Rosati, Director

Business model risk

"No matter what industry you're in, if you don't change, you'll lag behind. You need to understand the innovation challenges out there and adapt your business model as necessary. To manage business model risk, however, you need a clear understanding of who takes the lead—management, the board, the audit committee? What the business model should look like generally falls under board expertise, but the audit committee, with its understanding of financial drivers, should be able to do some pushing and prodding to ensure the right questions are being asked. Together, they can help ensure the business model remains relevant and in sync with or leading the industry and technological trends."

Harry Ort, Director

© 2016 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Introduction

Disruption on multiple fronts is putting audit committees on high alert

It has become one of the most commonly used terms in business today.

Virtually no strategic conversation proceeds without someone citing the need to either be disruptive or to respond quickly to disruptive market and industry trends—trends that have typically been connected to technology in one way or another. We don't, however, generally think about the concept of disruption when talking about the audit committee, even when we're discussing its changing role and responsibilities.

However, the concept of disruption is broadening its meaning beyond its current association with the interaction between technology, business and market forces. It is being applied in other areas and to other, broader trends. One might talk, for example, about the disruptive impact of demographic trends, rather than just technological ones. To that end, a high-level concept of disruption provides a valuable framework for discussing many of the changes and challenges currently facing the audit committee. And there are, without question, a range of audit trends that can only be seen as disruptive, given the kind of substantive change they are driving and their potential to transform the way audit committees do what they do—and what they are increasingly being asked to do.

Disruption can affect audit committees in different ways. In some cases—for example, cyber security—audit committees must become more knowledgeable and more vigilant in their oversight due to the rapid, ongoing evolution of the field. In other areas, such as oversight of reporting and compliance, it is their own approaches and processes that are changing, as complex standards up the global regulatory ante.

This report, as always, is about audit trends affecting the governance and oversight responsibilities of the audit committee. Our goal this year is to look at some of the more disruptive trends, at the ways in which they are driving or necessitating substantive change and at how audit committees are, or should be, responding.

© 2016 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

1. Technological risk

Technological disruption continues to appear on the audit committee agenda, with audit committees challenged to ensure they are considering the full-range of existing and emerging risks and that the appropriate technological knowledge and experience are represented on the committee.

Cyber security risk [1]

With cyberattacks on corporate networks and systems becoming more advanced, cyber security remains a major oversight concern for audit committees. Years ago, retail and financial services organizations were most at risk due to the processing of credit card data. Today, personal information is frequently targeted over credit card data, placing a much broader range of organizations at risk. The cyber security challenge can be broken into five more granular topics:

1. Data protection

Data protection, while clearly connected to cyber security, actually falls into a larger business security category, as data loss can occur in many ways. When considering data protection, audit committees often receive from management a list of security programs that are currently in place; however, the first step should really be making sure the right information has been identified and data sets clearly defined. This can be a challenge as what is considered relevant continues to change. Today, things like user names, passwords, awards program profiles and social media accounts are being targeted. Given that this list will continually evolve, audit committees should regularly confirm that the definition and protection of alternative data sets—beyond standard credit card information—is being carried out. To augment the information they have at hand, audit committees can also request relevant data directly from IT, for example, testing results, reviews of key data and hacking reports.

2. Social engineering

Social engineering is a broad term for any kind of psychological deception or exploitation of the "human factor" to gain access to information. Email phishing is one form, but attacks can be much more complex, employing phone calls, physical impersonation or any scenario that plays on the target's sympathy, fear, greed, etc. Proper oversight should involve social media acceptable use policies and organizational workflows detailing proper account usage.

3. Auditing of third-parties

Many organizations are relying more and more on third parties as part of their business model. The audit committee should ensure that management has considered and evaluated whether appropriate controls are in place to prevent misuse of any confidential customer information aggregated by third-party vendors. To be more certain that the organization is not creating additional liabilities, third-party audits are becoming more common.

4. Cyber insurance

Cyber insurance addresses an organization's liability when faced with cyber-based risks, such as a data breach or data destruction resulting in the loss of sensitive information. Organizations are beginning to purchase these types of policies, but there remains some confusion over exactly what is and isn't covered. The audit committee should have oversight over such policies in meeting with the insurer to confirm that the organization's significant financial exposures are, in fact, included.

5. Remediation procedures

Too often, audit committees look at a cyberbreach, ensure a particular, established process is being followed, then move on. More and more, however, we see audit committees getting involved in post-mortem follow-up reviews, sometimes even going beyond the standard oversight role in order to understand what went wrong, ensure remediation compliance and probe for other areas of vulnerabilities to help combat future attacks.

1 For further analysis of these and other current cyber security issues, read the KPMG publication "Cyber Watch Report: Be in a defensible position. Be cyber resilient." at https://home.kpmg.comcontent/dam/kpmg/pdf/2016/02/cyber-watch-report-en.pdf.

© 2016 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

"It's critical to ensure an industry-recognized risk management framework is in place that measures both the design and effectiveness of security controls. This will allow identification, tracking and management of cyber risk while tying it into your organization's larger risk management framework."

Kevvie Fowler,
National Cyber Response Leader

Business model risk

When an organization effectively implements an industry-changing technological innovation, one major effect is that their competitors' business models—and possibly a business model that has been an industry standard—can be disrupted. Consider the effect ride sharing has had on the way the taxi industry has been operating for decades or how Internet-based streaming services have changed the way television is purchased and consumed. Going forward, audit committees will need to pay greater attention to how, and which, disruptive technologies could potentially put the organization's business model at risk.

D&A privacy risk

D&A is changing business significantly and the organizations that are best leveraging it are seeing dramatic results. Like all disruptive technologies, however, there are corresponding risks, including increased privacy risk. Customers and other stakeholders entrust information to organizations for specific purposes, but those organizations may exploit that information in other ways using D&A. This creates significant privacy oversight challenges that audit committees need to be aware of and address.

Technology project risk

Despite the impact of the current economy on some sectors, organizations continue to undertake IT and strategic transformation projects. While many of these organizations have finance and risk and audit committees, IT committees are not yet common. This is a concern as some organizations lack proper IT experience on the board. As such, they are spending significant dollars on big transformation projects without the proper governance to protect or maximize the investment. At the same time, regulators like OSFI (Office of the Superintendent of Financial Institutions) are raising the bar in the area of IT risks and controls, signaling the fact that it's time for audit committees to address this as part of their risk portfolio.

© 2016 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

2. Political and economic risk

Political and economic risks are increasingly becoming audit committee agenda topics, with large enterprises implementing sophisticated models to analyze them.

Economic volatility

The global economic environment has become extremely complex, as have the implications for Canadian businesses. While there are distinct opportunities around mergers, consolidations, building synergies and cutting costs, both the dollar and commodity prices remain difficult to predict. Exporters and tourism may benefit, but mining and energy are suffering. Amid these conflicting trends and confusing economic data—where risk can be rapidly heightened or diminished depending on the sector—audit committees need to be cognizant of global volatility as it relates to their own organization's financial strategy.

Emerging markets risks

Canadian companies are looking to access emerging markets, but the question of how to play in those markets and what risks they raise is key. It's important to balance your exposure in good and bad times and given current economic challenges, audit committees may want to scrutinize their organizations' new market entry plans more carefully.

How will management mitigate new risks? Do they fully understand them? How effective are existing controls? Are more controls needed? And if the company already operates in volatile markets, should a review of risk management in those jurisdictions be undertaken?

Geopolitics

Syrian refugees, Middle Eastern conflict, China's economic sluggishness: the complexities abound. While some of these global issues are generating more traditional geopolitical risks, events such as the massive demographic shift created by the Syrian refugees—and the many pressures that they are creating in Europe—are different and should be addressed. Even though China's economy is growing faster than the rest of the world, international stock markets came to a virtual standstill when China's market dropped, significantly resetting global trade dynamics. Factor in the enormous uncertainty surrounding the US election and what impacts its result may have and its clear geopolitical instability needs to remain on the audit committee radar.

"With falling oil prices, a weak dollar and general political uncertainty around the world—consider the Middle East conflicts, European refugee issues, China slowing down and the UK possibly leaving the EU as just a few examples—exercising greater oversight over political and economic risk needs to become a priority for Canadian audit committees."

Kristy Carscallen,
Canadian Managing Partner, Audit

© 2016 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

"Audit committees are becoming more focused on regulators' auditor inspection results and how they can be translated into audit quality. Regulators, in turn, (particularly securities regulators) are looking to see whether audit committees are effectively making this happen. Turning this dynamic into demonstrable quality improvement results is something that should definitely be on the audit committee agenda."

John Gordon,
Canadian Managing Partner,
Quality and Risk Management

Industries in crisis and audit committee priorities

For some industries, the intrinsic question of disruption and risk has had to be put on the back burner. Audit committees and boards at oil and gas and mining companies are already dealing with large-scale disruption of the economic and financial models they rely on. Although issues such as cyber security and IT remain important, for these organizations, operational issues and corporate survival in the current economy are the most pressing challenges. Many audit committees have had to narrow their discussions to the going-concern level, looking at strategic and cost-cutting alternatives that can help them weather the economic storm.

These organizations are focusing on issues such as bank debt, capital management, financing, asset sales, talent management, impairments and cost reduction initiatives. However, cost and headcount reductions can have significant impacts that companies may not always foresee. Internal controls, for example, may be impacted as the individuals tasked with executing on them may have changed positions or left the organization completely. Audit committees should make sure they understand these potential impacts and are comfortable that remedial measures are in place.

Also, given the potential for impairments, organizations in survival-focused industries should be sure to focus on stress-testing programs and scenarios, and audit committees should be sure they oversee that process.

The economy is arguably healthier now than during the global financial crisis, but it's just as volatile. Organizations need to diligently run stress-test scenarios to determine exactly where they stand and what they should do going forward. For example, commodity-type businessses might stress-test against oil at $20 or $30, gold at $1,200, copper at $2, etc. Audit committees will, of course, need to stay on top of those issues.

© 2016 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

3. The evolution of corporate reporting

Much has been made of recent developments in corporate reporting and that focus will continue as changes are ongoing. The simple fact is, a lot more is expected around reporting—from regulators, from shareholders and from companies themselves.

Is the full range of risks being disclosed and adequately discussed, including those that go beyond the coverage in the financial reports and traditional MD&A? Are the right people around the table to ensure reporting quality? How reliable is the information being gathered and reported and how much value do—or can—investors place on it? Is there consistency around the way reports are being prepared, executed and reviewed to ensure they add real value? To help answer these questions, we have identified three trends to which audit committees should pay particular attention.

1. Integrated and strategic reporting

There is growing recognition that the range of issues and opportunities affecting long-term business value is much broader than can be reflected in a set of current-year financial measures. Companies' reports need to reflect this if they are to support investors' capital-allocation decisions effectively. Initiatives such as Integrated Reporting (IR) are intended to provide a basis to address this by refocusing reporting around an organization's business model and strategic priorities. The aim is to reflect the critical opportunities and challenges that affect the business—the same issues that management is dealing with on a daily basis within the organization.

This trend toward integrating various statutory and voluntary forms of corporate reporting—for example, reporting on areas such as long-term value creation and corporate responsibility[2]—becomes challenging to achieve while still creating an annual report that is lean and manageable. A Corporate Reporting Dialogue (CRD) has been formed to help respond to this challenge and bring together IR and other emerging frameworks in this area.[3]

Importantly, this push towards improved disclosure of non-financial information beyond the traditional annual report is becoming critical to the audit committee's reporting oversight mandate.[4]

2 To learn more about the state of non-financial reporting worldwide, see Currents of change: The KPMG Survey of Corporate Responsibility Reporting 2015 at http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Documents/kpmg-survey-of-corporate-responsibility-reporting-2015-O-201511.pdf

3 http://corporatereportingdialogue.com/

4 For more information on integrated reporting visit: https://home.kpmg.com/xx/en/home/insights/2013/04/integrated-reporting.html

© 2016 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

"There is a growing trend toward what is being called 'strategic disclosure.' While statutory reports have traditionally focused on historical financial information, many global governments and securities regulators now require some form of strategic reporting[5]. In such reports, the Board is responsible for discussing the main trends and factors likely to affect the future development, performance and position of the company's business. Non-financial key performance indicators are often included to highlight these trends and factors."

Bill Murphy,
Governance and Assurance Leader

2. Expanded audit reports
Audit committees will be impacted by the trend toward expanded audit reporting. Intended to improve audit quality and transparency, auditors will be required to describe key audit matters, including what audit work was performed in those areas. The expanded audit report will also provide more transparency into auditor and management responsibilities with respect to the financial statements. The intention is to have a report tailored to each company's specific circumstances, particularly with respect to the risk profile and the auditor's understanding of and response to those risks. Audit committees should continue to monitor developments with respect to expanded auditor reporting, including experiences in other jurisdictions and the standard-setting processes in Canada and the US.

3. Disclosure of operating and other performance indicators
Companies are increasingly distributing operating metrics that relate to volumes, capacity, growth or other indicators of performance that are of interest to the market. This information is often provided on a quarterly—or even monthly—basis. Audit committees should understand the nature of the information being provided, as well as the underlying processes, to ensure that the information is accurate, complete and prepared on a consistent basis.

5 See, for example, https://home.kpmg.com/content/dam/kpmg/pdf/2014/09/practical-guide-strategic-report.pdf

© 2016 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

4. The increasing complexity of the regulatory landscape

There is no question that the massive ongoing increase in global regulatory complexity has had a disruptive effect on Canadian companies and their audit committees. Indeed, that was done with the intention of preventing a recurrence of the last decade's global financial crisis.

Emerging regulatory issues and standards

There are a number of emerging regulatory issues and standards that audit committees should be aware of going forward:

IFRS 9 – *Financial Instruments*
The release of IFRS 9 completes a project launched by the International Accounting Standards Board (IASB) in 2008 in response to the financial crisis. The new standard includes revised guidance on the classification and measurement of financial assets, including a new expected credit loss model for calculating impairment and introduces a more principles-based approach to hedge accounting that is closely aligned with risk management. The mandatory effective date is January 1, 2018, however, the standard can be early adopted.

IFRS 15 – *Revenue from Contracts with Customers*
Recognizing the need for more consistency around revenue recognition, the IASB and FASB have released a converged standard to take effect in 2018. It will replace much of existing IFRS and US GAAP guidance.

IFRS 16 – *Leases* will fundamentally change the accounting treatment of leases for lessees establishing a single, on-balance sheet accounting model that is similar to current finance lease accounting. This standard will require companies to bring most leases on-balance sheet from 2019.

IFRS 4 – *Insurance Contracts*
The IASB is finalizing an amendment to IFRS 4, which would permit qualifying entities to temporarily defer implementation of IFRS 9 (with additional disclosures) or overlay an adjustment to re-classify some volatility from profit or loss to other comprehensive income.

Ensuring third-party adherence to regulatory mandates is becoming more important as organizations outsource more of their audit processes, particularly internal audit.

Anti-Money Laundering (AML) legislation is changing both globally and in Canada, with the financial and reputational consequences of non-compliance being significant. With regulators raising stringency around financial institutions' obligation to better "know their customers," audit committees should pay increased attention in this area.

Privacy legislation
The UK recently passed a privacy law holding that when a privacy breach or breach of consent happens to an organization with operations in the UK, it can be fined 2% of global revenues. Audit committees for organizations with UK operations should understand this rule and prioritize oversight to ensure compliance, while also being vigilant of generally increasing privacy legislation globally.

© 2016 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

"Even those regulatory initiatives that have yet to be implemented in Canada are important, as our regulators are closely monitoring global change and do not want to lag on key measures. Neither should audit committees."

Naveen Kalia,
Partner, Audit

The audit committee's role in improving audit quality

From the discussion of audit quality indicators and expanded auditor reporting, to how to assess professional scepticism—audit committees are trying to better understand the factors that determine a high-quality audit. They are paying attention to CPAB and PCAOB (Public Company Accounting Oversight Board) auditor inspection results and are more consistently taking regulator comments into account.

Still, audit committees struggle with how to really measure the quality of the audits they are getting. Going forward, there is a great opportunity for organizations, regulators and auditors to work together on these issues and create a more direct line between regulatory feedback and the actions organizations can take to ensure it's implemented.

The impact of global regulations on Canadian audit committees

It should be clear from the preceding sections that audit committees need to keep a close eye on global regulatory developments, not only those being enacted in Canada, but those that—due to strong support in the US or Europe may or are likely to be adopted in Canada at some point. Audit firm rotation provides a good example. Although it becomes effective in the EU in June of 2016, auditor rotation is not expected to be mandatory in North America anytime soon. Nonetheless, fully understanding its potential ramifications—and those of other impending global changes—is likely a good idea, particularly if you're an EU parent or subsidiary.

© 2016 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Conclusion

The disruption paradigm applies—now to manage the transformation

For the most part, disruption has been closely—almost inextricably—linked to the notion of technological innovation and its various impacts on business models and businesses themselves. In market-terms, disruption usually refers to a technological innovation that is so different and creates such a ripple in an existing model (sales, customer service, production, etc.) that everyone else is forced to change the way they do things just to catch up.

Is this so different from what is happening to the role of the audit committee? The issues we have discussed are real and either happening or pending—the ripples are growing—and audit committee members are indeed seeing their mandate transformed. In some ways, audit committees are having to do some"catch up" as it relates to these disruptive forces.

Going forward, managing inevitable change will be both an audit committee priority and a challenge and one that all audit stakeholders—C-Suite, management, auditors, regulators, shareholders and even the public—have an interest in facilitating.

© 2016 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Best practices

How can audit committees address today's most pressing challenges?

- ☐ **Discuss the impact of regulatory trends as early as possible.** Many regulations are enacted in the US and Europe well before Canada; monitor these developments with an eye toward their potential impact.
- ☐ **Revisit risk appetite and risk frameworks more frequently** in light of tried and true efficiency ratios.
- ☐ **Engage third-party advisers.** To gain perspective on complex topics, involve third-party professionals—for example, on cyber security, tax or valuation—in audit committee meetings and processes. The audit committee mandate is getting more and more complex—expanding your view can prove extremely valuable.
- ☐ **Ensure you have the right skillsets** on the audit committee with respect to required knowledge.
- ☐ **Conduct stress-testing and scenario planning** to determine the impacts—both positive and negative—that things like cyber attacks or economic volatility could have on your organization.
- ☐ **Consider implementing director education sessions.** Employing professionals in and outside the organization to help ensure audit committee members are knowledgeable about major risks.
- ☐ **Rely more on risk functions.** As an example, set up a separate risk committee that leverages insights from key internal risk professionals.
- ☐ **Focus more broadly on talent and human capital.** Audit committees have an obvious interest in the calibre and capability of those involved in the finance organization. However, considering the interdependencies between finance and operations, looking closely at the talent in other functions that are critical to the control environment is a good way to improve financial reporting.
- ☐ **Review internal controls focused on preventing and detecting fraud.** In tough economic times, people in challenging personal circumstances may do things they wouldn't otherwise do. Make sure there are no gaps in the controls you have in place to keep that from happening.

© 2016 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Director commentary

Targeting transformation

Integrated reporting

"I anticipate integrated reporting having the biggest impact on the audit committee mandate as it would substantially enhance long-term value creation. Currently, audit committees are so focused on ensuring that regulatory reporting requirements are fulfilled that the story of how the company is actually doing is often lost. Adding clearer and more concise messaging around the state of the business would be highly beneficial to investors/shareholders, creating value as a result."

Wendy Kei, Director

Technology project risk

"We believe technology risk will be critically important going forward given its impact on privacy and data protection in the health care sector, particularly with respect to major IT projects. For example, more than one hospital has had issues around their transition to e-health records. It's a major transformational project that has to be done, but since audit committees may not be involved in overseeing the project management, they are several steps removed from understanding specific technological risks, such as those around privacy. So as an audit committee, how do you best manage such risks while still trying to ensure the project achieves its objectives? It can be a very difficult assignment depending on availability of the right audit committee resources."

Harry Ort, Director

© 2016 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Director commentary

Targeting transformation

Best practices

"Getting the right expertise around the table—and knowing when it's time to reach out for it—is absolutely vital for today's audit committee. You often need expertise outside of financial, but that can present an issue since the committee remains financially focused. Looking to attract people with a financial focus from specialized industries—for example, a CFO from the technology sector—can help augment expertise while maintaining general financial acumen."

Deborah Rosati, Director

© 2016 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Contributors

Canada

Todd M. Buchanan
National Leader of Accounting Advisory Services
tbuchanan@kpmg.ca
416-777-8847

Kristy Carscallen
Canadian Managing Partner, Audit
kcarscallen@kpmg.ca
416-777-8677

John A. Desjardins
Partner, Audit
jdesjardins@kpmg.ca
604-691-3103

Reinhard Dotzlaw
Partner, Department of Professional Practice
rdotzlaw@kpmg.ca
416-777-3955

Kevvie Fowler
National Cyber Response Leader
kevviefowler@kpmg.ca
416-777-3742

John Gordon
Canadian Managing Partner, Quality and Risk Management
johngordon@kpmg.ca
416-777-3357

Philippe Grubert
Partner, Audit
philgrubert@kpmg.ca
514-840-2608

Naveen Kalia
Partner, Audit
nkalia@kpmg.ca
416-777-8340

Luzita N. Kennedy
Partner, Accounting Advisory Services
lnkennedy@kpmg.ca
416-777-3782

Doug A. King
National Data and Analytics Leader, Audit
dking@kpmg.ca
416-777-8358

Jeff G. King
Partner, Accounting Advisory Services
jgking@kpmg.ca
416-777-8458

Sukesh Kumar
Partner, Audit
sukeshkumar@kpmg.ca
604-527-3768

Brendan G. Maher
Partner, Audit
bmaher@kpmg.ca
416-228-7210

Mary Lou Maher
Partner, Audit
mmaher@kpmg.ca
416-777-3303

Silvia Montefiore
Partner, Audit
smontefiore@kpmg.ca
416-228-7211

Bill J. Murphy
Governance and Assurance Leader
billmurphy@kpmg.ca
416-777-3040

Doug W. Reid
Partner, Audit
dougreid@kpmg.ca
902-492-6013

John Stelter
Partner, Audit
jstelter@kpmg.ca
780-429-6511

Murray P. Suey
Partner, Audit
msuey@kpmg.ca
403-691-8474

Doron Telem
National Risk Consulting Leader
dorontelem@kpmg.ca
416-777-3815

United Kingdom

Jimmy Daboo
Partner, Audit
jimmy.daboo@kpmg.co.uk
+44 20 73118350

United States

Dennis T. Whalen
Partner, Audit
dtwhalen@kpmg.com
212-733-7413

kpmg.ca/audit

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

© 2016 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 12819

The KPMG name and logo are registered trademarks or trademarks of KPMG International.