



## The board and audit committee's role in IT governance

On June 27, 2011, members of the Canadian Audit Committee Network (CACN) met in Toronto to discuss how boards and audit committees are overseeing the increasingly complex risks associated with information technology (IT). Members were joined by Kathy Lisson, a partner in the advisory services practice of Ernst & Young, and Tony Ritlop, Ernst & Young's service line leader for the Canadian information technology risk and assurance practice. This document synthesizes key insights from the discussion.<sup>1</sup> For a list of network participants, see Appendix 1 on page 11.

### Executive summary

Recent technological advances have enabled companies to capture significant competitive advantages, but new technology has also complicated the IT programs of many companies and introduced unfamiliar risks. One member said, *"IT is one of our [company's] biggest advantages, but it's really introduced a lot of risk that the board isn't used to overseeing."* As members discussed their oversight concerns, successful practices, and lessons learned, three key issues emerged, which are summarized below and covered in more detail on the following pages:

- **Rapid advances in technology have introduced new business risks** (page 2)

New technology, such as cloud computing, and the proliferation of social media have introduced business benefits as well as new risks that challenge companies to rethink their risk-mitigation approaches, including data security and access-control processes. Cyber attacks have also matured into persistent threats to the intellectual property of governments and commercial businesses. These attacks, which often originate outside North America, are difficult to detect and often elude traditional IT security tools.

- **IT oversight is both a board and audit committee responsibility** (page 5)

Where IT oversight responsibility resides is unique to each company and depends on how central IT is to a company's competitive advantage. But members said that, in general, the board *"should be looking at the major IT issues that intersect with a company's strategy, and audit committees should be taking the lead on more tactical issues."* In the event of a major IT system implementation, some companies have convened a special board or joint board/management committees.

- **Boards and audit committees are enhancing IT oversight** (page 7)

Members said their boards have developed practices aimed at improving the board's understanding of technology and associated risks. Approaches include building relationships with the Chief Information Officer (CIO), enhancing their understanding of the IT program, and seeking out additional sources of IT expertise. For a list of IT-related questions that audit committees might consider, see Appendix 2 on page 12.

<sup>1</sup> VantagePoint reflects the network's use of a modified version of the Chatham House Rule whereby names of members and their company affiliations are a matter of public record, but comments made during the meetings are not attributed to individuals or corporations. Quotes in italics are drawn directly from comments made by CACN members before and during the June 27 meeting; unitalized, unattributed quotes are drawn from discussions with audit committee chairs in other audit committee networks. Quotes from guests are attributed and unitalized.



## Rapid advances in technology have introduced new business risks

New technology often promises great benefits to companies, but it also complicates IT governance. Ms. Lisson and Mr. Ritlop said boards and audit committees should be aware of four trends: the threat of systemic intellectual property theft, cloud computing, social media, and the impact of emerging technologies on security-access controls.

### Advanced persistent threats pose significant risks

Ms. Lisson defined an advanced persistent threat as “a specific adversary which is tasked with collecting intelligence from Western military, government, and commercial organizations through ongoing attacks on computer systems.” She said, “These are not typical hackers ... [but rather] well-funded, well-organized groups, typically state sponsored, that hack into and monitor their targets for extended periods of time in order to extract intellectual property over a number of years. They were initially focused on government entities and companies in the defense industry, but now they are targeting firms in just about every industry.” Ms. Lisson explained that these attacks are especially difficult to detect because “they are going after specific files that reside on a company’s storage devices and extracting them right through the network. To find them, you need to monitor the data traffic on your network, looking for large data movements.” Even more troubling, industry experts say companies’ “traditional defenses don’t provide adequate protection” against advanced persistent threats.<sup>2</sup>

As a result of such attacks, Ms. Lisson explained, some Western companies “are seeing products being developed in other countries that look like their own. They are linking it back to attacks that happened 10 years ago.” To combat these attacks, Ms. Lisson and Mr. Ritlop recommended that companies “balance their resistance measures among prevention, detection, and incidence-response efforts.”

### The audit committee should understand the costs and benefits of cloud computing

Ms. Lisson defined cloud computing as “using the Internet to access someone else’s software running on someone else’s hardware in someone else’s data center.” Benefits of cloud computing include the convenience of accessing information from any location, rapid provision of services, lower unit costs for data storage, and secure backups to prevent data loss. Cloud computing is also helping companies avoid large capital investments, maintenance costs, and hassles. Ms. Lisson said, “The cloud is on-demand, broadly accessible, and elastic.” One audit chair remarked, “*You could have five servers today and 500 tomorrow.*” Given the benefits, cloud computing has become increasingly prevalent. According to a 2010 Ernst & Young survey, 45% of companies used or were planning to use cloud-computing services in the next 12 months,<sup>3</sup> a figure that surprised many members.

Still, cloud computing presents risks and potentially hidden costs. Ms. Lisson and Mr. Ritlop commented, “The data on these cloud servers is pooled, so your data will be sitting right next to someone else’s[data] and there is no physical segregation. Also people working at the cloud provider with administrative access can see all the data on any server. Some companies are concerned that cloud service providers could provide their data at the request of law enforcement or other governmental agencies, without the company’s

<sup>2</sup> William Jackson, “Are Advanced Persistent Threats Here to Stay?” *Defense Systems*, April 1, 2011.

<sup>3</sup> Ernst & Young, “Borderless Security: Ernst & Young’s 2010 Global Information Security Survey,” (Ernst & Young Global Limited, 2010), 8.



knowledge. In this case, the concern is not that the data has been provided – since companies would obviously comply with any lawful request – rather that the request could be made without their knowledge.” One member was concerned about *“the ability to access data a company places on a cloud.”* Ms. Lisson acknowledged data access can be an issue in the event data needs to be recovered because most cloud providers “do not offer prioritization of data recovery.” Of specific concern to audit committees, she also noted that given the newness of the cloud-computing industry, monitoring the accuracy of user invoicing (for cloud services buyers), and revenue recognition (for sellers) is essential.

Ms. Lisson said, “I think [cloud computing] will transform the industry, but it is still immature in resolving access and recovery policies right now.” One member agreed, saying, *“We need to understand the risks, but the benefits are significant. I’m going to ask our CIO if we’re using the cloud enough.”*

### **The audit committee should ensure there are clear policies on social-media use**

Last year Burson-Marsteller’s annual social-media survey found that 79% of the largest 100 companies in the Fortune Global 500 were using at least one form of social media – such as Twitter, Facebook, YouTube, or corporate blogs – to broadcast corporate messages.<sup>4</sup> This year, the survey found that companies were not just unilaterally broadcasting their own messages, but also directly and actively engaging with users.<sup>5</sup> In addition to helping companies engage with customers, social-media sites can also enable employees to be more innovative and productive.<sup>6</sup> Still, social media poses threats to company data. Ms. Lisson explained, “Employees can be leaking information whether they intend to or not. Restricting social-media sites like Facebook in the office does little to protect companies anymore – an employee could take a picture of a screen with their phone and post it to a site.”

In addition, document aggregation sites such as Docstoc, Scribd, and SlideShare encourage users to post policy documents online. Ms. Lisson noted, “Docstoc has publicly said they want to be the YouTube of professional documents sites. If you search your company’s name and the term ‘confidential,’ you’ll probably find confidential documents.”

This new age of social media mandates new policies for its use. Ms. Lisson and Mr. Ritlop advised creating a comprehensive yet clear policy that has consequences for misuse: “Policies need to be updated to include social-media and tablet use. They also have to have teeth. If no one is being challenged by line managers, the policies are probably not good enough.”

### **Data security and access controls are increasingly important**

Access-control issues are not new, but as the number of systems in a company grows, access control becomes increasingly complex and difficult to monitor. Ms. Lisson said, “The priority used to be giving the right access to the right people at the right time. Now, it’s the reverse: the number-one priority should be making sure the wrong people have the wrong access removed at the right time (“deprovisioning”).” One

<sup>4</sup> Burson-Marsteller, “2010 Fortune Global 100 Social Media Study.” *The Burson-Marsteller Blog*, February 23, 2010.

<sup>5</sup> Burson-Marsteller, “2011 Fortune Global 100 Social Media Study.” *The Burson-Marsteller Blog*, February 15, 2011.

<sup>6</sup> Kristin Burnham, “Social Media Safety: Acceptable-Use Policies Are Critical.” *CIO*, April 8, 2010.



member said, “Access controls are so dependent on human interaction. Many employees say their managers don’t even know what systems they have access to.”

These risks are magnified with the number of mobile devices that have access to companies’ networks. An audit committee chair in another network noted, “We recently took inventory on the number of mobile devices that our employees have. We have about 7,000 employees. We found that those 7,000 employees have about 31,000 devices which can access the network.” Ms. Lisson said, “One of the biggest changes companies are making to improve access control is implementing role-based access [policies], rather than creating unique access for each employee. They are also requiring IT departments to explain to managers in plain English the access they are approving for their employees.”

Companies can also run afoul of access controls when employees leave the organization. An Ernst & Young survey found 75% of respondents “are concerned (33% are very concerned) with the possible reprisal from employees recently separated from their organizations.”<sup>7</sup> One member noted, “There seems to be a business model issue. IT and HR don’t communicate effectively enough when someone leaves.” Another commented, “It’s not just employees; contractors also have access to all sorts of systems.” Members agreed better communication between these two groups would drastically improve the access-control process.

Ms. Lisson and Mr. Ritlop said access-control exceptions for senior executives can sometimes be problematic: “Executives can be granted access to systems that they may not even realize they have. They are also usually allowed to access confidential material from their homes or iPads.” One member added, “Board members are similar in that we have a lot of confidential information stored on our tablets.”

### Questions for the CIO

Ms. Lisson, Mr. Ritlop, and several members suggested questions that directors should ask the CIO about new and emerging technology risks:

- What are our most valuable information assets? How are we protecting these assets from advanced persistent threats? How are we monitoring the network for large packages of data moving out of our corporate systems?
- What percentage of our IT budget is dedicated to IT risk and security?
- What is our cloud strategy? Is it appropriate for all of our business units? What is the exit strategy if something should happen with the cloud provider? How do our traditional outsourced service providers compare with cloud providers in terms of costs, benefits, and risks?

*continued overleaf*

<sup>7</sup> Ernst & Young, *Outpacing Change: Ernst & Young’s 12th Annual Global Information Security Survey* (Ernst & Young Global Limited, 2009), 6.



### Questions for the CIO *continued*

- What is the current inventory of cloud services in use? What policies do we have in place regarding the purchase of cloud services by individual businesses or functions?
- What access-level exceptions do our executives have? Are the executives using the access they are provided? How does their access affect the risk profile of the company? How are we protecting company information when they access it from home?
- What are our policies regarding use of social media? When were the policies updated? How clear and effective are they?
- When was the last time the communications and/or internal audit team searched major social-networking and document-aggregation sites for leaks of confidential information or comments about the company or its executives that could hurt the company's brand?
- Have we performed tabletop exercises for major incidents or breach of information? What are the worst-case scenarios?
- Have we hired third party firms to test the strength of our security defenses? Are these firms using both automated and manual processes to penetrate our systems?

### IT oversight is both a board and audit committee responsibility

Oversight of IT is unique to every company, and several members agreed that oversight structure *“really depends on how closely IT is related to the strategy of the company or how important it is to maintaining competitive advantage.”* One member suggested, *“IT should be on the board and the audit committee agenda. The board should delegate some [of the oversight] to the audit committee, including IT reports coming from internal audit, but the big risks and trends need to be discussed at the full-board level.”*

Regardless of where oversight resides, members stressed the importance of making the distinction in duties explicit. In a limited number of cases, boards have created a special committee to oversee IT projects demanding close board supervision.

### Boards have broad oversight of IT

Many members agreed that the full board retains the majority of IT oversight responsibilities because *“IT can be so integral to the strategy that it has to be considered at the board level.”* One member explained, *“We talk about IT at the board level in terms of tying it into the strategy and growing our competitive advantage or losing our competitive advantage if we’re not moving fast enough.”* The member added, *“You can’t talk about IT strategy alone. It’s tied to your sales strategy, your operating strategy, and your management strategy.”*

While many members agreed that the board should be responsible for the overarching IT strategy, some boards are also taking responsibility for overseeing major IT projects: *“The board tends to look at [IT] with*



*an eye to timeliness and budget. In that respect, IT projects have not been treated differently than large capital projects ... The board will hear about the IT project through updates and see if it is on time and on budget ... [The project] is very rarely reviewed [in depth] unless there is a problem, though."*

### **Audit committees typically have specific IT oversight responsibilities**

Members said the audit committee's oversight of IT is generally more focused on the "processes and controls around IT" and the "more tactical issues." Given their proximity to the financial statements, members said the audit committee is best positioned to "understand how [financial] reporting and internal controls could be affected by IT issues." Other members said audit committees can have a larger IT oversight role, but it is "extraordinarily industry and company dependent." Regardless of the extent of the audit committee's oversight, many members said IT has been elevated on their audit committee agendas. As evidence, one member remarked, "Information-security reports used to be at the back of the audit committee book. Now they are at the front."

However, some members are concerned that increased responsibility for IT at the audit-committee level has the potential for "diluting the oversight capabilities" of the committee. One member explained, "Although [IT] might reasonably fit with [the audit committee], it doesn't have to be there." Another member noted, "At some point, someone has to put a wall around what the audit committee oversees. If it keeps increasing, we'll start overseeing anything with any level of risk."

### **Special-committee oversight of IT is predominantly ad hoc**

A number of members explained that their companies have convened special committees to oversee certain aspects of IT. Benefits of involving qualified directors in such committees, according to members, include "great guidance for management" and candid reporting back to the board, especially during in-camera sessions. Members described two primary special-committee responsibilities:

- **Major systems projects.** Members said that boards rarely meet frequently enough or have enough time to closely oversee IT projects, so in some cases boards are forming special committees tasked with monitoring major IT undertakings. One member explained, "[IT] projects can get out of hand quickly if they are not kept on track. A committee dedicated to overseeing the progress really helped the comfort level of the board."
- **IT strategy.** One member's board "established a special committee to focus on new technology strategy." At another member's company, the special IT committee "is comprised of board members and management that work with the relevant people in management" and spearhead the oversight of IT programs.

In one unique case, a member's board created a committee to oversee large capital projects, which encompasses IT projects: "We have an oversight committee that looks at big capital projects, and this committee would review a big IT project. The committee is off duty when there is not a project. [It is comprised of] board members and management, and they report back to the [full] board."



## Boards and audit committees are enhancing IT oversight

According to a *Harvard Business Review* case study, “Regulatory changes have affected the composition, role, and responsibilities of Boards of Directors worldwide. While stronger frameworks for directors’ fiduciary responsibilities have resulted, considerably less attention has been devoted to understanding the nature of, and concomitant duty-of-care toward, the information systems and technology assets in the organization, or IT Governance. As a result, Boards have not demonstrated the competence or attention that good IT governance demands.”<sup>8</sup> Some members agreed, with one saying, “*We don’t look at IT as much as we should [at the board level] – it’s relatively underrepresented.*” Yet many members said their boards and audit committees have adopted practices that allow them to have a better understanding of their companies’ IT programs.

## Building a deeper relationship with the CIO

Acknowledging the lack of IT expertise on the board, many members said directors depend on the CIO to “*raise the right issues and give us the right information.*” Yet many CIOs still lack stature within the executive management team: “Chief information officers are more important than ever to the success of their companies, given the crucial role information technology has come to play in every aspect of business. But in most companies, the CIO still isn’t viewed as a peer by other senior executives, who tend to see CIOs as specialists lacking the full set of broad management skills.”<sup>9</sup>

While members agreed this can be the case at certain companies, many believe that a new generation of CIOs are emerging that “*bridge the gap between technology and the business,*” and this is helping to elevate the role of the CIO. Indeed, one member said, “*The CIO has more visibility now. He has a seat at the [executive] table.*” Members suggested that those CIOs enjoying more elevated roles are ones who have “*business experience and leadership qualities*” rather than just extensive IT knowledge. One member said, “*A great CIO has the ability to communicate to the board in a way that gives us confidence that they are thinking about not just yesterday’s problems, but also how to progress the strategy of the company. They are good business people first and tech experts second.*”

The level of interaction the CIO has with the board and audit committee often depends on how important IT is to the business model and strategy. Some members said their companies’ CIOs only present to the board annually (if that often), while others said the CIO comes to almost every audit committee meeting. The majority of members agreed with one who said, “*I think we should be seeing the CIO more often.*” Another member remarked, “*I’d like to better understand the demands, challenges, and competing priorities my CIO is dealing with ... I need to spend some time building that relationship.*”

Members discussed two ways to build the CIO relationship:

- **In-camera sessions at board meetings.** One member said, “*I think boards should have [a private] session with the CIO. Boards could ask, ‘Are you properly resourced and are you getting support from the management team?’ My experience is that this [conversation] does not happen.*”

<sup>8</sup> Michael Parent and Blaize Horner Reich, *Governing Information Technology Risk* (Boston: Harvard Business School Press, 2009).

<sup>9</sup> Peter S. Delisi, Dennis Moberg, and Ronald Danielson, “[Why CIOs Are Last Among Equals.](#)” *Wall Street Journal*, May 24, 2010.



- **Informal interactions.** One member said, *“I’m going to take the CIO to lunch and ask him some of the [issues] we’ve talked about today.”* Another added, *“I have not had [informal] meetings with my CIO before, but I am going to start having them.”*

### Enhancing IT program evaluations

Several members shared approaches their boards and audit committees use to better understand and evaluate their firms’ IT programs, suggesting that boards and audit committees take the following actions:

- **Understand how IT supports business objectives.** New IT initiatives should be driven predominantly by the business units rather than the IT department: *“It’s business units that should be looking at their strategy and pushing for the new tools that they need. IT should be working alongside the business leaders, enabling [the business units] to be successful by providing them with the [technological] tools they need. If the business units are not driving this process, they won’t use the tools correctly or fully.”*
- **Seek proactive reporting.** Members said IT reports are too often *“reactive”*: *“[Boards] only receive IT information after a breach.”* Instead of reactive reports, some committees are seeking reports that provide updates on *“improvements IT is making, [in addition to] the three latest threats on the company.”* At one member’s company, *“The CIO and head of [human resources] present a combined report to the board. They talk about the [IT] trends as well as what the needs are for both the systems and the skill sets we will need for the future.”*
- **Question IT budgets.** Without having to understand each line item of the IT budget, boards and audit committees can get a feel for the appropriateness of the budget by asking questions like, *“If you had X percent, more or less, what changes would you make?”* Mr. Ritlop also suggested asking, *“What percentage of the IT budget is spent on security?”* He added, *“Companies with world-class information security are spending 8% to 10% of their IT budget on security.”*
- **Solicit user feedback.** Seeking feedback directly from the *“customers”* of internal IT systems, such as business unit leaders, gives the board more insight into the IT program and the value it produces. One member said, *“You should be talking to the business unit heads to understand where their frustrations are and where they are pleased with the [IT program].”*

### Leveraging internal and external expertise

Members agreed that many directors *“simply do not have the expertise to understand the full scope of IT risks ... IT can seem like a black box sometimes.”* As such, members suggested resources boards and audit committees could use to enhance their understanding of IT:

- **Internal audit.** Internal audit is a resource for identifying IT issues, particularly those related to *“financial systems and internal controls.”* With a view of all areas of the business, it is well positioned to identify individual risks that could signal systemic risk if viewed together: *“Internal audit kept running into access-control issues [across business units]. Instead of 17 small problems, they consolidated them into one issue and it rose to the level of a significant deficiency.”* However, as one member said,



*“Internal audit can be limited by their lack of deep IT knowledge.” To address this, one member’s company uses a co-sourcing model that draws on the deep IT expertise of a Big Four accounting firm: “We’ve been using a co-source model and it’s been hugely effective because the outside firm has brought in specific [IT] expertise. [Co-sourcing has] really elevated the thinking and helped link IT to the strategy.”*

- **External auditors.** Several members suggested that external auditors could provide the board and audit committee with more IT insight. One member suggested that external auditors should *“advise the board on what [the emerging trends are], what [the board] should be thinking about, and what questions [the board] should be asking.”*
- **Third-party tests of IT security.** Several members said their companies have used so-called “ethical hackers” – IT firms hired to penetrate company systems and uncover weaknesses – to help understand specific vulnerabilities. Most members agreed that these types of experts *“provide a good check on what management says they have secured.”* However, one member questioned whether the board should hire these hackers themselves: *“Hopefully the board [would have to bring in a hacker] only on an exception basis.”*
- **Other outside advisors.** One member suggested, *“Boards should have a strong outside third party they can look to when they think they need more information.”* Some companies are using the IT advisory services of auditing firms: *“We’ve used audit firms to augment our internal audit teams when they were looking at IT projects.”* One audit committee chair from another network remarked, *“We brought in [an auditing firm] to go through and take a look at the IT security area. They came back with three suggestions and helped management develop an IT scorecard, which the audit committee is keeping track of.”* However, members agreed that bringing in outside advisors is *“not a common solution – it’s something boards seek when there is a comfort issue.”*
- **Directors with IT expertise.** Most boards do not have directors with specific IT expertise, but one member’s board made it a component of their desired skill set: *“We consider [IT expertise] as part of our director qualifications. We always have it on our skills matrix, though it’s never been top of the list ... Having someone with that sort of expertise is more important now than it ever has been.”* Still, one member said, *“[Director candidates] with IT expertise are hard to find because you ideally want someone that is still [a sitting executive in an IT role or at a technology company] ... They are few and far between.”*



## Conclusion

One recent Ernst & Young study predicted, “By 2014, more smart devices – portable tools that connect to the internet – could be used to access the internet than traditional computers.”<sup>10</sup> In the same study, one consultancy also predicted that by 2016, all Forbes Global 2000 companies will use cloud services.<sup>11</sup> This not-so-distant future will require even more advanced oversight of IT. How will the board keep up with these technological advances and the risks they pose? Will director education and support from internal and external resources be enough, or will boards need directors with direct IT experience? As one member said, “*IT has really become a driver of our business, but we still don’t have any high level of IT expertise at the board. I’m not sure we need it right now, but I could see that changing.*” The time to seek out greater IT expertise on the board may be closer than many directors think.

## About this document

The Canadian Audit Committee Network is a group of audit committee chairs drawn from leading companies committed to improving the performance of audit committees and enhancing trust in financial markets. The network is convened by Ernst & Young and orchestrated by Tapestry Networks to access emerging best practices and share insights into issues that dominate the new audit committee environment.

*VantagePoint* is produced by Tapestry Networks to stimulate timely, substantive board discussions about the choices confronting audit committee members, management, and their advisers as they endeavor to fulfill their respective responsibilities to the investing public. The ultimate value of *VantagePoint* lies in its power to help all constituencies develop their own informed points of view on these important issues. Anyone who receives *VantagePoint* may share it with those in their own network. The more board members, members of management, and advisers who become systematically engaged in this dialogue, the more value will be created for all.

*The views expressed in this document represent those of the Canadian Audit Committee Network. They do not reflect the views nor constitute the advice of network members, their companies, Ernst & Young, or Tapestry Networks. Please consult your advisers for specific advice. Ernst & Young refers to all members of the global Ernst & Young organization, including the US member firm of Ernst & Young LLP.*

*This material is copyrighted by Ernst & Young and prepared by Tapestry Networks. It may be reproduced and redistributed, but only in its entirety, including all copyright and trademark legends.*

---

<sup>10</sup> Ernst & Young, *Tracking Global Trends: How Six Key Developments Are Shaping the Business World* (Ernst & Young Global Limited, 2011), 21.

<sup>11</sup> *Ibid.*, 22.



## **Appendix 1: Meeting participants**

The following network members participated in the meeting:

- Bev Briscoe, Audit Committee Chair, Goldcorp
- John Caldwell, Audit Committee Chair, IAMGOLD
- Peter Case, Audit Committee Chair, Fortis
- John Clappison, Audit Committee Chair, Sun Life Financial
- Alan Horn, Audit Committee Chair, Fairfax Financial Holdings
- Michel Labonte, Audit Committee Chair, Metro
- David Leslie, Audit Committee Chair, Enbridge
- Eileen Mercier, Audit Committee Chair, CGI Group
- Bob Steacy, Audit Committee Chair, Domtar
- Barb Stymiest, Audit Committee Chair, Research in Motion
- Ron Tysoc, Audit Committee Chair, CIBC
- Paul Weiss, Audit Committee Chair, BCE

Ernst & Young was represented by the following:

- Richard Greisch, Partner, Assurance Services, Ernst & Young
- Tom Kornya, Managing Partner, Greater Toronto Area, Ernst & Young Canada
- Kathy Lisson, Partner, Advisory Services Practice, Ernst & Young Canada
- Tony Ritlop, Service Line Leader, Information Technology Risk and Assurance Practice, Ernst & Young Canada
- Rob Scullion, Managing Partner for Assurance and Advisory Business Services, Ernst & Young Canada

The following members took part in discussions before and/or after the meeting:

- Tom O'Neill, Audit Committee Chair, Loblaw
- Jane Peverett, Audit Committee Chair, EnCana
- Ted Reevey, Audit Committee Chair, Bell Aliant
- Stuart Smith, Audit Committee Chair, Yellow Pages Income Fund



## Appendix 2: Questions for audit committees

- ? What IT issues and trends are having the greatest impact on strategic and tactical decision-making at your company? Which present the biggest challenges and the greatest opportunities?
- ? How are important IT issues and risks changing over time?
- ? What have been the most significant changes to technology policies in the past few years?
- ? How are IT oversight responsibilities shared among the full board, the audit committee, and other committees? How has the audit committee's role in IT oversight changed in the last few years?
- ? Under what circumstances would your board consider forming a permanent or temporary board-level IT committee?
- ? Has the amount of time your board has spent on IT issues increased, decreased, or stayed the same in the last 12 months? What changes do you anticipate in the next year?
- ? What are the signs that a company has the right CIO, and what red flags suggest that it might not?
- ? How often does the CIO present to the board or audit committee? What information is presented? What additional information would be helpful?
- ? How can the board gain insight into the bench strength and vulnerabilities of the IT organization? How important is it for the board to understand succession planning for key IT professionals?
- ? What sources of technical expertise are helpful to boards and audit committees as they consider IT issues? What should the board expect from the external audit firm in this regard?
- ? How could internal and external experts provide better support to the board or audit committee for IT oversight? What are the barriers to increased support?
- ? Is your company seeking greater IT expertise on the board? What additional IT education is provided for directors?