CANADIAN
AUDIT COMMITTEE NETWORK
VantagePoint

April 30, 2007

TAPESTRY NETWORKS, INC · WWW.TAPESTRYNETWORKS.COM · +1 781-290-2270

Information technology governance

Introduction

The Canadian Audit Committee Network is a select group of audit committee chairs drawn from leading Canadian companies. 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 evolving audit environment.

The third meeting of the network was held in Toronto on April 3, 2007, and focused on practical ways for boards and audit committees to effectively address the growing risks and opportunities arising from information technology.

This document reflects a synthesis of the key issues that emerged from the meeting. The ultimate value of *VantagePoint* lies in its power to help all constituencies develop their own informed points of view on important issues such as these. Anyone who receives this publication may share it with those in their own network. The more broadly we can disseminate this information to board directors, management executives, and their advisers, the greater the value created for all.

Between them, the members of the network who participated in the meeting sit on the boards of over 30 large-, mid-, and small-cap public companies. The attendees were:

- Mike Boychuk, Audit Committee Chair, Yellow Pages Income Fund
- John Caldwell, Audit Committee Chair, Cognos
- Denis Desautels, Audit Committee Chair, Alcan
- Don Fullerton, Audit Committee Chair, Husky Energy
- Krystyna Hoeg, Audit Committee Chair, Sun Life Financial
- Bob Luba, Audit Committee Chair, MDS
- Tom O'Neill, Audit Committee Chair, BCE
- Pierre Robitaille, Audit Committee Chair, Gildan Activewear

Also attending the meeting from Ernst & Young Canada were:

- Anne-Marie Hubert, Risk Advisory Services Partner, Canadian Technology Security Risk Services
- Lou Pagnutti, Area Managing Partner; Chairman and Chief Executive Officer
- Rob Scullion, Managing Partner for Assurance and Advisory Business Services

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.

Executive summary

IT governance is a "framework that supports the effective and efficient management of information resources (e.g., people, funding, and information) to facilitate the achievement of corporate objectives. The focus is on the measurement and management of IT performance to ensure that the risks and costs associated with IT are appropriately controlled."[1]

Members of the Canadian Audit Committee Network agreed that the strategic and operational importance of IT justifies board attention. Given the role of technology in financial reporting and controls, audit committees often take a leading role in IT oversight. Members discussed the risks and opportunities created by IT, considered the division of responsibility between the audit committee and the full board, and identified internal and external sources of expertise that they could rely on.

- **Information technology oversight must consider both risks and opportunities** *(page 3)*

  The growing deployment of information technology systems is creating immense opportunities, and almost equal risk. The implementation of Section 404 revealed unexpected weaknesses in IT controls. While the audit committee has primary responsibility for financial reporting risks, boards must also consider the impact of information technology on strategy and operations.

- **Boards must ensure IT oversight responsibilities are appropriately assigned** *(page 4)*

  Members identified a need for a division of responsibility on the board with regard to IT oversight. The audit committee has a clear responsibility for IT systems that support financial reporting. However, audit committees already carry a heavy workload and cannot be responsible for all IT discussions. If technology is a key strategic driver for the business, members believe the full board should be actively engaged in IT oversight. If, however, IT systems support, but do not drive, corporate strategy, then members do not believe full board involvement is warranted.

- **Audit committees must rely on external and internal sources of IT expertise** *(page 4)*

  Although few audit committee members have deep IT expertise, they can draw on the expertise of others. The external audit firm, the internal audit function, and the CIO can all provide guidance and advice and help to create a comprehensive picture of the IT function. Additionally, some members saw value in increasing IT expertise on the board to make sure the right questions are being asked.

Following the meeting, Ernst & Young prepared an extensive list of questions for board directors to consider as they pursue various IT governance objectives. Topic areas include: achieving tighter alignment between the business and IT; managing IT investment to achieve value; addressing compliance requirements; measuring performance; developing and implementing a consistent risk management framework; developing the right organization and resource management; and, ensuring effective governance over third parties. This list can be found in the appendix on page 7.

[1] Ken Doughty and Frank Grieco, "IT Governance: Pass or Fail?" *Information Systems Control Journa*l 2, 2005. Available at http://www.isaca.org/Template.cfm?Section=JOnline&CONTENTID=24195&TEMPLATE=/ContentManagement/ContentDisplay.cfm.

Information technology oversight must consider both risks and opportunities

Large companies depend on effective information technology to support complex operational and control systems. Mission-critical systems have to operate as intended and without disruption, and financial systems must deliver information that is accurate, reliable, timely and secure. For these reasons, IT oversight is increasingly becoming an issue for corporate directors.

Not only is *"information technology increasingly responsible for both opportunities and threats,"* but it is also *"increasing in importance [because of the] amount of the capital budget"* represented by system implementations and upgrades. In the light of IT's importance, members expressed concern over the lack of attention IT oversight has historically received from many boards. In many cases, full-board discussions of IT address capital expenditures only, and not broader issues of IT governance.

Members agreed that IT governance falls broadly into three buckets: financial reporting, operations, and strategy.

- **Financial reporting.** Many companies discovered unanticipated IT issues during their recent internal controls certification. A recent article in *Compliance Week* noted, "disclosures ranged from problems with security and segregation of duties to documentation of steps and procedures and the manual transfer of information among programs or applications, in addition to other woes."[2] Members expressed surprise at the number of manual work-around procedures that were identified in their own companies. Some felt that, in many ways, *"[Sarbanes-Oxley Section] 404 was the audit committee's best friend."* Issues for the audit committee to consider include access and program change controls, documentation of IT policies, and other general controls such as back up and recovery, scheduling, incident and problem management. Members described financial reporting and control risks as important elements in the company's enterprise-wide risk management framework.
- **Operations.** Companies are increasingly relying on IT systems to support mission-critical operational processes, including manufacturing, sales, and supply chain management. While these operations don't fall directly within the oversight responsibilities of the audit committee, successes or failures will have a significant impact on the financial results of a company. Boards need to consider key questions, including: Can we manage change to our IT environment without exposing our company to unacceptable risks? Can we keep our systems secure from internal and external threats? Can we be efficient and cost effective? And can we articulate objectives and get value from our IT investment?
- **Strategy.** For some companies, IT is a key driver of corporate strategy, and there can be *"competitive disadvantage being behind the cutting edge."* For other companies, IT is merely a tool that supports the business. Boards may view IT as a source of opportunity rather than as an area of business risk, but *"it's a significant challenge [to] align IT with business strategy."*

[2] Tammy Whitehouse, "Where IT, Internal Controls Collide," *Compliance Week,* October 17, 2006. Available at http://www.datablueprint.com/documents/interviews/20061017_whereitinternalcontrolscollide.pdf.

Boards must ensure IT oversight responsibilities are appropriately assigned

Members eagerly discussed the question *"Who takes ownership of IT at the board level?"* The audit committee takes a leading role in some key areas of IT governance, especially around systems that support financial compliance and disaster recovery (a component of the committee's risk oversight responsibility), since disaster recovery is not within the scope of Sarbanes-Oxley Section 404. However, members were clear that the audit committee should not bear full responsibility for IT oversight associated with operations and strategy. As one member noted, *"On the audit committee, we have too much work and can't take on the whole thing."*

Strategic discussions belong to the full board

Members felt that for industries in which IT is a strategic driver, the full board should be very engaged, and the audit committee should drive that engagement. They cautioned, however, that the nature of the board's engagement, even when IT is a strategic driver, will vary with the industry and the impact of IT.

If IT is not a strategic driver for the company, members questioned whether the full board should ever devote time to IT. In such cases, members felt that the board need only consider significant IT expenditures, just as it would any other major capital project.

The audit committee deals with IT risks related to financial reporting

Audit committees find themselves dealing with IT both proactively, by reaching out to address some issues, and reactively, as issues are brought to them:

- **Proactive.** Many audit committees are reaching out to the IT function to help with compliance issues, while fewer are ensuring that disaster recovery plans are sufficient.
- **Reactive.** Members noted that information technology issues *"creep into the audit committee in the report of the internal auditor."*

Members agree that security failures and compromises around privacy *"can be cataclysmic."* Not only must the company deal with the specific issue at hand, it must also deal with the reputational impact. On the other hand, members pointed out that IT issues are rarely, if ever, a key component of corporate fraud. *"The number of frauds caused by bad IT?"* one member asked rhetorically, and then answered, *"None."*

Audit committees must rely on external and internal sources of IT expertise

Members acknowledged that few board directors have deep IT expertise. It is therefore important for the directors to engage with experts in order to adequately understand the relevant issues and alternatives. Members noted that often the *"external auditor and internal auditor will provide information on [the IT] function's performance and issues."*

Additionally, there is desire among CIOs without direct access to the audit committee to have more frequent interaction. In an interview for *InSights*, one CIO stated, *"The audit committee chair is well-informed of the issues, but it wouldn't hurt to sit down from time to time to share information."*[3]

External auditor

Audit committee chairs can discuss IT matters with the accounting firm's IT experts on the audit team to ensure that committee members understand the IT environment and the related risks, controls, and any control gaps that may exist. Members said external audit firms offer several advantages as a source of IT expertise: (1) they understand the company's business and organisation, (2) they know how IT impacts controls and other risk areas, and (3) they have the resources and skills to provide a current perspective on IT risks, challenges, and opportunities.

Members noted that *"your external auditor will take you some of the way"* in addressing IT governance issues, particularly those that relate to financial reporting and regulatory compliance. However, a holistic view of the IT function is not typically within the scope of an audit engagement.

Internal auditor

Internal audit can provide directors with a more complete picture of the IT function. *"With the right internal resources,"* one member noted, internal audit can provide you with useful *"second opinions."* However, despite the important role of internal audit in IT governance, members noted that *"good internal audit staff are hard to keep."* Another agreed: *"You need the function, but you can't keep the [IT] resources [in-house]."* In practice, IT internal audit is frequently outsourced to a third party.

Expanding the board's relationship with the CIO

While CIOs are increasingly playing a vital role across all business units and functions, they don't appear to be growing in visibility with the board. Directors who recognize the importance of the CIO and the IT function also recognize that *"the CIO has to get more air time on the board and with the audit committee. They have to make more of a contribution and have more accountability."*

As a result of the network meeting, one member made a commitment to *"put the CIO on the list of people I see more frequently."* Another noted that the rise in importance of IT at the member's own company will help *"kick off a conversation with the CIO."* Members who don't already see the CIO on a regular basis agreed that they *"need to get that expertise"* and the knowledge and comfort that comes with it.

Does the audit committee need to have answers, or questions?

Members realized that complicated issues such as IT governance *"may raise more questions than answers."* Boards operate with a measure of uncertainty on most issues. The question for directors is how to fulfill their corporate governance responsibilities without crossing the "bright line" between oversight and management.

---

[3] Ernst & Young and Tapestry Networks, "The CIO's perspective," *InSights,* February 28, 2005, 7. Available at http://www.tapestrynetworks.com/documents/Tapestry_EY_ACLN_Feb05_InSights.pdf.

According to a survey by Burson-Marsteller, in 2004 only 8% of Fortune Global 500 companies had a current or former CIO on the board.[4] Members are divided as to the value of IT expertise on the audit committee. In a pre-meeting interview, one member cautioned that having an apparent IT expert on the committee does not necessarily add the experience necessary for oversight: *"I have been on a board with a very high-ranking IT executive, and frankly, I thought [their] oversight and input [were] pretty much like the rest of ours. [They] didn't drill down into detailed questions."* However, other members believe that current or former IT executives can add significant value. As one member remarked, *"The board has the challenge [of seeing] if those running things are competent,"* and directors with IT expertise *"allow us to be more hands-on in the audit committee."*

Members identified several next steps and immediate actions

- *"See the CIO more."* Members believe audit committees would benefit from more formal and informal interactions with the CIO.
- *"Get the right resources."* The external auditor, internal auditor, and IT consulting firms can help round out directors' understanding of IT governance practices and issues.
- *"Get a better handle on IT governance."* Members say boards should engage in a more comprehensive discussion to ensure IT risks are understood and IT oversight responsibilities are assigned.
- *"Add IT knowledge to the board member skill gap analysis."* Some members felt companies should consider adding IT skills to their skills matrix, much as financial expertise was added in response to Sarbanes-Oxley.

Conclusion

In a world in which *"IT is pervasive,"* companies are experiencing new opportunities and risks associated with information technology. Clear communication and strong relationships must exist to make sure that there is no governance overlap and that nothing is overlooked.

Even though few directors consider themselves IT experts, they can draw on many sources of expertise to guide their actions. And by acknowledging that sometimes they will have more questions than answers, audit committee chairs can become comfortable discussing IT in the same way they have become comfortable with other, more traditional audit committee discussion topics.

[4] Burson-Marsteller, *A Missing Competency: Boardroom IT-deficit* (Burson-Marsteller, 2005), 4. Available at http://www.burson-marsteller.com/pdf/IT_Deficit_2005_Brochure.pdf.

Appendix: Questions for boards to consider as they pursue IT governance objectives[5]

Assessing the alignment between the organizations business and IT objectives

Objectives

Reach an understanding and agreement between business and IT about IT's role and the business contribution. Get senior management in both IT and the business involved and accountable for IT governance and supportive of the board in setting direction.

Key questions to ask

- Is there clear board-level accountability for IT in your organisation?
- What training does the board receive to enable effective and confident discussion of IT? How confident are board members about initiating and maintaining that IT discussion?
- Do board members understand the IT spend and it's link to the business strategy and objectives? To what extent is there common understanding of what IT value means?
- Can board members articulate and agree on a set of critical IT assets and risks? Are the areas of interdependence between IT and business risks clearly identified? How confident are you that risks are being addressed consistently across the organisation?

Overseeing management of IT investment to achieve value

Objectives

Apply robust governance to evaluate proposed new initiatives, prioritize them, and monitor progress. Ensure project goals and objectives remain consistent and that expected benefits are achieved, whilst allowing for changing business needs and risks that are inevitable during lengthy programs. Understand the cost drivers and issues in IT, the extent and nature of budgets and spend, and how spend is monitored.

Key questions to ask

- Are the board, IT management, and finance in alignment about how to articulate, measure, and monitor IT costs and value?
- How is business stakeholder buy-in and accountability for new system investments and business benefits achieved?

[5] Prepared by Ernst & Young following the April 3, 2007, Canadian Audit Committee Network meeting as a resource for audit committees and other board directors.

- Is there a formal and rigorous portfolio evaluation approach for potential new projects? Is it consistent, well understood, and does it recognize the need for multiple evaluation criteria according to the specific program?

Addressing compliance requirements

Objectives

Have a framework and process to ensure compliance requirements are identified and addressed efficiently and effectively. Be confident that the appropriate IT related controls are in place to understand and comply with the myriad of IT-related compliance requirements in an efficient manner.

Key questions to ask

- Are you confident that you really understand the implications of IT-dependant compliance programs such as SOX 404, MI 52-109, IFRS, and EU 8th directive?
- Do your internal and external advisors assess and report to the board on compliance with IT related regulatory requirements?
- Is there an enterprise-wide and formal approach to ensure awareness of forthcoming compliance requirements and compliance with at least minimum requirements?
- Is there clear accountability for achieving and maintaining compliance? Are results reported to the board on a regular basis?
- How do you embed compliance in the organisation once the initial work to achieve it has been completed?

Ensuring performance is measured

Objectives

Increase the likelihood that the perception and reality of IT's performance and contribution to the business will be in alignment. Have confidence that sound investment decisions are being made based on the availability of accurate and relevant information. Achieve visible agreement by all stakeholders on what is important and craft a framework within which measures can be adjusted as the business evolves and success criteria change.

Key questions to ask

- Is there an agreed-upon business view of successful IT performance? Do you have discreet measures for large strategic IT investments?

- How have you determined what to measure, and have you ensured that you have the necessary measurement tools and processes in place? Do you receive reporting as to performance against these measures?
- What actions are taken as a result of IT performance measurement?
- Is the approach to measuring IT integrated with the approach and timing for measuring business performance?
- Does your measurement framework provide for changes in business priorities and therefore changes in IT performance measures?

Developing and implementing a consistent risk management framework

Objectives

Have a visible means whereby individuals can raise concerns and identify red flags. Gain confidence that programs are on track to deliver accurate reports of risks. Have clear criteria for go/no-go decisions at critical stages in the program and the support to change or stop failing programs on a timely basis.

Key questions to ask

- Is there a clearly articulated and well-understood risk management approach across the enterprise? Is it applied to IT?
- When did you last see a comprehensive IT risk assessment? Was it independently verified?
- How confident are you that risk assessment and management is a real core competency across the organisation?
- How confident are you that a rigorous approach is taken to categorizing IT risks? Once risks have been categorized, do only the high risks get discussed?
- How do you measure the effectiveness of your risk management strategies and activities?
- Is risk management truly embedded in the organisation, or is it regarded as the domain of auditors and compliance?

Developing the right IT organisation and resource management

Objectives

Have formal and regular assessment of the IT organisation, both to achieve value from IT expenditure (on human, technological, and financial resources) and to make the right trade-offs between costs and risk when making IT sourcing strategies and decisions. Be confident that the IT organisation is cost effective, that it delivers systems at costs that are comparable with industry leaders, using well-trained and skilled staff, and that it is effective at resource balancing. Provide a structure within which resources, recruitment,

compensation, and benefits can be assessed. Understand early warning signals of potential mismatch between IT capability and desired business goals. Maintain the ability to manage outsourcing arrangements.

Key questions to ask

- How do you align your IT organisation with your strategy?
- When did you last justify the numbers and balance of skills of people in your IT organisation?
- When did you last carry out a rigorous organisational capability assessment?
- How does your IT organisational capability influence your sourcing decisions?
- How do you justify your IT training budget? Is it aligned with your IT strategy?
- How easily, and at what cost, can sourcing decisions be reversed or changed after they have been made?

Ensuring effective governance over third parties

Objectives

Clearly articulate and agree on objectives and standards from the start and support them with well-constructed contracts aligned with specific requirements. Have a governance framework that addresses the full outsourcing cycle. Ensure thorough due diligence and set key performance indicators before deals are signed.

Key questions to ask

- Are key stakeholders agreed on the primary and secondary objectives for working with a third party? Is it to increase efficiency, cut costs, gain access to skills, or to support step change in the organisation?
- Is there a good cultural fit between your organisation and the potential third party? Does the third party organisation maintain similar values?
- Are there clear criteria and mechanisms to measure success?
- How confident are you that you have the skills to manage the third-party relation effectively?
- Is responsibility and accountability clearly defined, documented, and understood, both within your organisation and that of the third party?
- Do you receive the appropriate level of assurance from third party providers as to their compliance/performance with the key compliance/risk measures embedded in the agreement?