PACIFIC SOUTHWEST
AUDIT COMMITTEE NETWORK

VantagePoint

July 20, 2007

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

Information technology governance

Introduction

The Pacific Southwest Audit Committee Network is a group of audit committee chairs drawn from leading companies based in the Pacific Southwest region of the United States. The network held its seventh meeting on June 21, 2007, to discuss the topic "Information technology governance." IT governance can be defined as a leadership, strategy, and "framework that supports the effective and efficient management of information resources (e.g., people, funding, and information) to facilitate the achievement of corporate objectives."[1] This document is a synthesis of insights and comments from that meeting.

Members also participated in an unreported open session, during which they discussed other issues, including whether the audit chair should delegate any items to other members of the audit committee, the emerging relationship between the audit committee and the compensation committee, and Auditing Standard No. 5, which was issued recently by the Public Company Accounting Oversight Board.

The members of the network participating in the meeting sit on the boards of about 20 large-, mid-, and small-cap public companies. They were:

- Joe Bronson, Jacobs Engineering Group
- David Engelman, Fleetwood Enterprises
- George Farinsky, Broadcom Corporation
- Mike Fisher, Insight Enterprises
- Diana Laing, The Macerich Company
- Marty Melone, Countrywide Financial

Ernst & Young participants in the meeting were:

- Gary Birkenbeuel, Managing Partner, Pacific Southwest Area Assurance and Advisory Business Services
- Ed Chavannes, Senior Manager, Technology and Security Risk 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. Network members' remarks appear in italicized quotes.

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

Executive summary

The Pacific Southwest Audit Committee Network's discussion focused primarily on ways in which the audit committee properly oversees information technology risk. The following important ideas were discussed:

- **Board involvement in oversight of information technology is expanding** *(Page 2)*

  Information technology governance is handled differently in every company and is often linked to the strategic importance of IT to the business. In some companies IT governance is overseen by the full board, in others by the audit committee or another board committee. At senior levels in the organization, the importance of IT is often indicated by whom the CIO reports to: the CEO, CFO, or others. In companies with strong acquisition strategies, smooth IT integration is considered critical and strong performance by the IT function is required.

- **Information technology risks are not limited to IT controls** *(Page 4)*

  Members feel that Sarbanes-Oxley Section 404 has given public company boards added confidence in the IT controls associated with financial reporting. But many IT risks remain: how vulnerable is equipment to the risk of theft, and how secure are confidential materials? What recovery plans are in place to keep IT functioning in the event of a disaster? While companies report significant financial investment in IT, they also report difficulty tracking progress and return on the investment.

- **Boards and audit committees can draw on many sources of IT expertise** *(Page 5)*

  Although few audit committee members have deep IT expertise – by one survey, less than one in ten Fortune Global 500 companies have a former CIO on the board – they can draw on the expertise of others. The external audit firm, the internal audit function, and outside specialists can all provide guidance and advice and help to create a comprehensive picture of the IT function.

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 business and IT objectives, managing IT investment to achieve value, addressing compliance requirements, measuring performance, developing and implementing a consistent risk management framework, developing the right IT organization and resource management, and ensuring effective governance of third parties. This list can be found in the appendix on page 7.

Board involvement with information technology is expanding

IT governance is moving up the corporate agenda, propelled by several trends, including the increasing cost and complexity of IT systems, the scale and growth of Internet-enabled businesses, the need for IT-related compliance, and the increasing risk of cyber attacks from outside the enterprise.

Members began the meeting by considering some sobering statistics. According to research provided by Ernst & Young:

- 40% of IT spending brought no return to the organization.

- 84% of large organizations experienced at least one major security breach in the past year.
- 26% of companies in 2007 planned to increase outsourcing over 2006 levels.
- IT spending averages $6,700 per employee per year.
- Only 20% of IT spending is on the growth of systems, while 80% is on maintenance of current systems.

Members reported differing roles for the board in IT oversight:

- **Board does not provide oversight.** Some members reported that, while they understood the importance of information technology, at their companies *"boards don't spend any time on [IT governance]."* One member noted that, unfortunately, *"boards and audit committees don't do much with IT, period."*
- **Board does provide oversight.** However, other members agreed with one audit chair who said, *"Audit committees can deal with [some] problems [and] other committees can deal with [other] problems, but ultimately the [full] board has to deal with IT, as it is very connected to long-term strategies."* However, even those boards that are reviewing IT often make do with an annual presentation from the CIO or with the IT portion of a wider enterprise risk management report. Another member said that at the very least, boards should be concerned with *"IT controls and risk, and, in the case of fast-growing companies, infrastructure. If you don't get infrastructure right, the whole thing can break, so a lot of attention is paid to that, to scalability."*

  Members agreed that when boards have taken oversight responsibility for IT, in practice this responsibility is often delegated to the audit committee. Even when the board reviews and approves the strategic IT plan, the audit committee is generally charged with the ongoing oversight of any tactical activities, including mitigation of IT-related risks.

One member noted that when IT is considered a strategic issue, risks may be addressed in multiple board and company forums: *"IT is highly involved [as a] value-add for the business. [The audit committee] meets with the IT head twice a year, [who meets] another three times with the full board, and it's highly visible because it's integrated into the business and the customers. It's part of that fabric, part of our value-add for customers."*

The strategic importance of IT is reflected in reporting relationships and executive focus

While members agreed that IT is becoming increasingly important, they acknowledged that exactly how important it is varies widely by company and industry. One member asked, *"Who does the CIO report to? To me, that's an indication of what influence IT has in an organization."* According to recent data from a *CIO* magazine survey of more than 500 CIOs, "forty-one percent (41%) of CIOs report directly to the CEO while only 24% report to the CFO, consistent with last year's findings … Sixty-eight percent (68%) of CIOs surveyed sit on their organization's business executive management committee."[2]

[2] *CIO* magazine, *The State of the CIO: Highlights from* CIO *Magazine's annual, definitive research into the state of IT leadership* (Framingham, MA: CXO Media, 2007), 1. Available at http://www.cio.com/state/stateofcio.pdf.

Similarly, members cited senior executive attention as a significant driver of IT in an organization. *"With our CEO,"* one member remarked, *"we talk at every meeting about CIO-related topics."*

Information technology is critical for successful acquisitions and integrations

Members on the boards of highly acquisitive companies reported needing a robust and agile IT infrastructure with the ability to merge with, or replace, the IT system in an acquired company. One member noted that integration was their biggest IT challenge: *"We have an acquisition strategy. Acquire and swallow, including their IT systems. Depending on the size of the acquisition, integration is extremely important, [as are] controls."* Another audit committee chair agreed, stating, *"If you're going to put your system into an acquired company, your system had better be pretty good. [We have] templates with measurements on how we're doing and how things are being implemented."*

One member remarked that at the member's company, the IT function had developed significant experience with integrations: *"They know what they're going to do, as opposed to figuring it out as they go."* Another agreed, stating, *"We have a very good integration capability. You have to. Management know what they're doing because they do the same thing, every time ... IT is always embedded in the process."*

Information technology risks are not limited to IT controls

Corporations depend on IT to support complex operational and control systems. IT systems have to operate as intended and without disruption, and financial systems must deliver information that is accurate, reliable, timely, and secure. A failure in these systems – through a failed implementation, a security breach, or a loss of physical hardware – can cause significant disruption to company operations.

Members feel that Sarbanes-Oxley Section 404 has given public company boards added confidence in the IT controls associated with financial reporting. One member said, *"If the company is not doing a good job, you have to demand it, or IT will become a material weakness."* However, comfort levels decrease as boards consider other aspects of information technology. Members see value in increased dialogue between the board and the IT function, including the CIO.

The many forms of IT risk

Members explained that IT risk takes many forms, from highly organized external attacks on their networks to more basic security breaches like *"somebody grabbing a laptop."* As companies are increasingly obtaining and recording confidential information (including credit card numbers and other personal data), members wondered, *"How do you know you have that data locked down?"*

Additionally, members said the board's responsibility for IT governance often includes issues related to business continuity. One member asked, *"How do you know your data center isn't going to be the next one on fire or flooded? Business continuity needs to be assessed – that [risk] could be substantial."* One member spoke of the need to separate processing centers physically, especially given the risk of earthquakes in California: *"We have two data centers, one in northern California, one in southern California. We back those up at least daily. If we had a calamity, a natural disaster, we could recover."*

Addressing IT risks requires defense in breadth, a coordinated effort that secures all the systems and data in a company. As one member noted, a security effort, *"like many things in business, doesn't work right unless it works together."*

Sometimes IT issues also emerge from enterprise risk management or other internal risk assessments. One member said, *"Our risk-based internal audit plan usually identifies two to three IT issues a year."* These are then tracked by the internal audit function.

Tracking progress and measuring returns on IT investments

Members agreed that major IT projects have traditionally presented challenges for management and boards. One member observed, *"Most [IT] projects end up over budget, or fail."* When asked what metrics were used to measure return on IT investment, one member said, *"I have an easy answer: none."*

While some companies lack metrics to measure IT performance, others use basic financial measures. One member explained, *"We look at the budget at the full board and audit committee level: capital expenditure budgets, personnel, the new systems that are coming up, and their implementation. It's pretty rudimentary. The board approves the budget, but [the audit committee] digs into it a little deeper than the board. The board gets it rolled up through the controller, who presents the plan. The CIO attends [the meeting], and can comment and answer questions."*

Another member described a process that relied on measuring progress toward project deadlines. *"We look at the implementation schedule. [One current] implementation will take four or five years, and we have all these [project] plans around. It's very visible and measurable. It's not rocket science; it's 'Are you doing it? Have you met this benchmark? If not, why? Was it changed?' That's pretty simple."*

Boards and audit committees can draw on many sources of IT expertise

Members recognize that while the practical responsibility for IT governance often rests with the audit committee, audit committee members generally lack IT expertise. Indeed, 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.[3] In such cases, the audit committee and the audit chair often turn to other sources of expertise both inside and outside the company for guidance and comfort.

Internal audit may provide expertise

"If IT is important," one member stressed, *"then you have to spend the money to get [IT expertise] into your internal audit group."* Members felt that good internal auditors can provide directors with a complete picture of the IT function and can also serve as a useful second opinion on issues that the CIO presents.

Members agreed that it is extraordinarily challenging to find and retain internal auditors with IT expertise. These professionals are *"hot property,"* and hiring them is *"very difficult."* One member who had been

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

involved in the search reported, *"We couldn't find the right person outside."* Another noted that the solution they came up with was to *"outsource for IT help [to] supplement our own IT expertise."*

Experts outside the company can also provide valuable advice

Audit committees can also look outside the company for guidance. One member remarked, *"There are plenty of people to turn to,"* and another noted that *"all the major [accounting] firms are qualified"* to provide guidance in this area.

In addition to issue-specific advice, outside vendors can also be engaged to give an independent, comprehensive review of the IT function. Regarding such a review, one member remarked, *"I imagine it would be valuable, but I'd like the CEO to [direct] it, not the board."* Asked if an independent comprehensive review would be beneficial, a member stated, *"You don't get an answer to that [question] until it's done."* Members who supported the idea also cautioned that it came with a possible downside: *"[IT] is pedaling so fast, if [the review] takes them away from mission-critical tasks, then we're not helped."*

Conclusion

For many firms, IT is increasingly becoming *"the engine that drives the business,"* but the new opportunities IT creates also bring with them new risks. Clear communication and strong relationships must exist to make sure that nothing is overlooked in IT governance efforts.

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, much as they have become comfortable with other, more traditional audit committee discussion topics.

The views expressed in this document represent those of the Pacific Southwest 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 counselors for specific advice. Ernst & Young refers to all members of the global Ernst & Young organization, including the U.S. member firm of Ernst & Young LLP.

Appendix: Questions for boards to consider as they pursue IT governance objectives[4]

Assessing the alignment between the organization's business and IT objectives

Objectives: Reach understanding and agreement between business and IT about IT's role and its 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 organization?
- 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 its 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 organization?

Overseeing management of IT investment to achieve value

Objectives: 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 the inevitable changes in business needs and risks that arise 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?
- Is there a formal and rigorous portfolio evaluation approach for potential new projects? Is it consistent and well understood, and does it recognize the need for multiple evaluation criteria according to the specific program?

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

Addressing compliance requirements

Objectives: Have a framework and process that ensure compliance requirements are identified and addressed efficiently and effectively. Be confident that the IT-related controls in place will permit comprehension of and efficient compliance with the myriad of IT-related compliance requirements.

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 advisers 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 organization 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 accurate and relevant information. Bring all stakeholders into agreement on what is important, and craft a framework that permits measures to 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 discrete 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 on 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. Have confidence that programs will deliver accurate reports of risks. Have clear criteria for go/no-go decisions at critical stages in the program and the ability 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 organization?
- 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 organization, or is it regarded as the domain of auditors and compliance?

Developing the right IT organization and resource management

Objectives: Have formal and regular assessment of the IT organization, both to achieve value from IT expenditure and to make the right trade-offs between costs and risk when making IT sourcing strategies and decisions. Be confident that the IT organization 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 organization with your strategy?
- When did you last justify the numbers and balance of skills of people in your IT organization?
- When did you last carry out a rigorous organizational capability assessment of your IT organization?
- How does your IT organizational 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 of 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 organization?
- Is there a good cultural fit between your organization and the potential third party? Does the third-party organization 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 organization and that of the third party?
- Do you receive the appropriate level of assurance from third-party providers regarding their performance as measured by the key compliance and risk measures embedded in the agreement?