

IT risks and governance

Introduction

On June 29, 2006, members of the Audit Committee Leadership Network (ACLN) met for the network's 13th meeting. Members began by considering information technology (IT) governance and the associated technology risks; they then explored in depth another particular source of risk: pension obligations.¹

Members focused on three aspects of IT governance during their discussion:

- **Three key IT-related risks**
- **Sources of expertise for the audit committee and the board**
- **IT oversight by the audit committee and the board**

Audit chairs participating in the meeting included:

- Gene Fife, Audit Committee Chair, Caterpillar
- Roland Hernandez, Audit Committee Chair, Wal-Mart
- Judith Richards Hope, Audit Committee Chair, Union Pacific
- Chuck Noski, Audit Committee Chair, Microsoft and Morgan Stanley
- Sandy Warner, Audit Committee Chair, General Electric Company
- Steve West, Audit Committee Chair, Cisco Systems

Audit chairs who participated in individual discussions before the meeting were:

- John Clendenin, Audit Committee Chair, The Home Depot
- Shirley Ann Jackson, Audit Committee Chair, Marathon Oil
- Marie Knowles, Audit Committee Chair, McKesson
- Peter Ueberroth, Audit Committee Chair, The Coca-Cola Company
- Doug Yearley, Audit Committee Chair, Lockheed Martin

The members listed above sit on the boards of over 40 large-, mid-, and small-cap public companies between them. Other members participating in the meeting included:

- John Ferraro, Vice Chairman, Ernst & Young
- Tom Flannery, Partner and Director, Audit Committee Communications, Ernst & Young

ViewPoints 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 before and during meetings are not attributed to individuals or corporations.

¹ See Audit Committee Leadership Network, "Pension obligations: a deep dive into one area of risk," *ViewPoints*, July 19, 2006. Available at: http://www.tapestrynetworks.com/documents/Tapestry_EY_ACLN_July06_View14.pdf

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.”²

IT risks and governance are moving up the corporate agenda, propelled by several trends, including the need for IT-related compliance, the increasing cost and complexity of IT systems, reliance on vendor IT, and the increasing risk of attacks from inside or outside the enterprise.

- **Three key IT-related risks** (*Page 3*)

Members identified three key IT-related risks confronting their companies that they deal with via the audit committee or the board: (1) compliance and controls risk, partly prompted by the implementation of Section 404; (2) business continuity risk, especially in the wake of 9/11 and, more recently, Hurricanes Katrina and Rita; (3) security and privacy risk, which are also seen as important contributors to reputation risk. Audit chairs are struggling to find appropriate metrics to measure the impact of all three key IT-related risks on the company. [Questions for the audit committee to ask management about IT-related risks can be found on pages 4 and 5.](#)

- **Sources of expertise for the audit committee and the board** (*Page 6*)

Most members reject the idea that the board should appoint directors who are technology specialists; they see such a specialty as too narrow to contribute across the whole board agenda. Instead they rely on the expertise of specialists in the external and internal audit teams. Advisory boards are also a popular method of making external expertise available to boards and audit committees. Those members who favored the idea of putting specialists on the board tended to identify people who had gained technical expertise during earlier careers and who are “CEO-like CIOs.”

- **IT oversight by the audit committee and the board** (*Page 7*)

Members report two different approaches to audit committee oversight of IT: the board may delegate oversight of IT governance (including technology risks) to the audit committee, or the audit committee may have responsibility only for specific IT risks, which are often related to financial data.

As for board oversight of IT, most members agree that the board’s responsibility for disclosure and controls requires the board to provide at least a minimum level of oversight. However, members reject a one-size-fits-all model for board oversight. Some members’ boards provide regular oversight of the IT function; others limit oversight to discussions of IT risks; still others just conduct ad hoc reviews of particularly sensitive IT projects. Although some members’ companies have board-level technology committees, and there appears to be a growing trend to create such committees, most members are skeptical of their value. [Examples of technology committee objectives can be found on page 9.](#)

² 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>

Three key IT-related risks

Information technology can create both opportunity and risks for any business. While IT often appears on the board agenda as an enabler of opportunity (for example, to improve customer service or reduce costs), the audit committee tends to focus more on IT risks.

Members identified three key IT-related risks:

- 1. Compliance and controls risk– can we rely on the integrity of information?
- 2. Business continuity risk – can we keep the business running?
- 3. Security and privacy risk – can we keep the bad guys out?

1. Compliance and controls risk – can we rely on the integrity of information?

IT reliability is critical to financial reporting. In larger companies, numerous internal controls are handled as part of the IT system. Many audit chairs are concerned about the continuing prominence of manual systems and general lack of automation. One member said, “[Our] IT [systems were] more basic than we’d like to admit,” and confessed a need to “get rid of the hardware store mentality.”

According to leading CIOs interviewed for *InSights* last year, “Section 404 brought discipline to the implementation and documentation of essential controls, a more uniform application of policies, and an identification of gaps in processes.”³ Several ACLN members agree with this view. Speaking before the meeting, one member said, “[Section] 404 really helped to set up the agenda for IT.”

Companies also need to understand the risks associated with dependence on vendor IT, even when there is little actual outsourcing. One member said Hurricane Katrina drove home the fact that “you can have great data systems and backups, but if there are no telecoms in place, it doesn’t matter.” Another member admitted, “I don’t know anything at all about the vendors we use. Yet if the vendor goes down, that can harm a big chunk of the business.”

Due diligence for vendors is critical, as are very specific service-level agreements. Several members with experience of large capital projects said they insisted on having IT and the internal auditors conduct an audit of IT suppliers before any outsourcing contract was signed. They also insisted on regular audits from their internal auditors after the contracts were agreed.

2. Business continuity risk – can we keep the business running?

Members said the experience of 9/11 had prompted management to prepare new business continuity plans that included distributing IT systems and building in redundancy to mitigate against the risk of similar events in the future. Terrorism had been the catalyst for often delayed capital investments. Some members mentioned that IT vulnerabilities had only come to light after 9/11.

³ Ernst & Young and Tapestry Networks, “The CIO’s perspective,” *InSights*, February 28, 2005, 2. Available at: http://www.tapestrynetworks.com/documents/Tapestry_EY_ACLN_Feb05_InSights.pdf

The CIO of a Fortune 50 company we spoke with in preparation for this meeting said he would ask audit chairs, “How much are you assuming the public infrastructure will be there, and how long can you wait for it? Assured communications weren’t there for [Hurricane] Katrina or 9/11. If we had depended on public infrastructure, we would have waited two to three weeks for support from the government.” This CIO also suggested asking about plans for employee recovery: Where will employees come from to do the recovery work? Will those employees be able to make it to a backup site if there is no transport?

One member said, *“I cannot imagine a company of any scale that does not have a business continuity plan around IT. Now, whether it is able to be implemented is a different thing. If you have a site go down, can your plan really protect you or give you the backup?”*

Business continuity: questions for the audit committee to ask management

- What plan is in place for dealing with significant business interruption?
- What kinds of crises or business interruptions are you prepared for?
- When did you last test this? What didn’t work as expected?
- What is the maximum volume that backup systems can handle?
- What level of redundancy is required, and at what cost?
- How long will recovery take?

3. Security and privacy risk – can we keep the bad guys out?

One aspect of security was singled out by audit chairs as being of particular concern: privacy. One member commented, *“This is a big issue, especially customer data. How we use it, how it is accessed, and how it is gathered. It is a larger ... concern than the other [risks].”* Another audit chair said privacy also represented a reputation risk, in terms of how the company would recover from a serious breach.

- **External security risks.** The CIO interviewed before the meeting commented, “In the world of cyber warfare, it’s not about hackers but about international experts paid by foreign governments ... They may already have been in your systems for a year taking the information they want.” This CIO believes very strongly that in the next 12–18 months shareholders will force boards to ask questions about IT security as there will be “an Enron-sized event impacting a major company, and a lot of others will be exposed or under pressure.” One member commented, *“IT security is a very big issue ... Our networks are constantly being hammered. It only takes a few people to get access to a corporation.”*
- **Internal security risks.** Only one in 12 of the CIOs interviewed for *InSights* identified external threats as the biggest IT risk area. Ten thought internal access controls were the biggest risk.⁴ Members tended to agree. One commented, *“When probed on security risk, our [IT leadership] felt they had a grip on [external threats]. They were more worried about our own people.”*

⁴ Ibid., 5.

IT security and privacy risk: questions for the audit committee to ask management

- If the network has been violated, how would you know? Do you know what to look for?
- At what level, and with what degree of sophistication, are you monitoring for violations?
- Has the company employed third parties to attack and penetrate the company's technology infrastructure? What has changed as a result?

Another possible IT-related risk: failure to get value for money from IT projects

Speaking before the meeting, an IT consultant said that for most large companies, IT spending is “the third-largest expenditure, [measured] as a percentage of operational and capital expenses. The board or audit committee should seek value for money. But boards rarely get as involved with IT failures as they would if it was a factory failure.” Members of the European Audit Committee Leadership Network identified failure to get value for money from IT projects as a significant IT-related risk at their May 2006 meeting.⁵

Most U.S. members do not spend any time on project delivery in audit committee meetings. One member commented, *“If there is consistent under-delivery or failure, management should deal with it and the board and audit committee [should] oversee that. But we don't oversee any other capital expenditure projects.”* Another member agreed: *“I have not seen a board being engaged with project delivery and efficiency. Isn't it a management responsibility, like marketing? It is tough for the board to engage in operational issues.”* However this was not a universal view. One member said, *“When you are spending large amounts of shareholders' money, we do ask if we are getting value.”*

Project delivery: questions for the audit committee to ask management

- How does the IT strategy support the business, and how are investment decisions made?
- What impact do our IT investments have on shareholder value and share price?
- Does our IT platform accommodate growth and change?

Measuring IT risks

Audit chairs are struggling to find appropriate metrics to measure the impact on the company of all three key IT-related risks. One member asked, *“How do we [develop] metrics we can use to track progress or deterioration over time?”* This member suggested one approach: *“We benchmark with the best in class and make it fully transparent to the audit committee,”* but remarked, *“It feels subjective and qualitative, too IT driven and not external enough. The audit committee is not satisfied yet.”* Another audit chair said, *“We rely on functional experts to give us a sense of the risk. Internal audit can be helpful. External audit gets more attention, and we want an external perspective.”*

The latest version of COBIT 4.0 (Control Objectives for Information and related Technology), an IT control framework, focuses on measurement. The chairman of the Information Systems Audit and Control Association (ISACA), which develops COBIT, said, “Part of getting value, and being able to measure what

⁵ See European Audit Committee Leadership Network, “IT governance,” *ViewPoints*, May 30, 2006, 7. Available at: http://www.tapestrynetworks.com/documents/Tapestry_EY_Euro_ACLN_May06_View8.pdf

you're getting, is identifying the right kinds of measures that you can use to monitor IT performance."⁶ The measures developed include treating IT investments like other investments and managing them similarly.

Sources of expertise for the audit committee and the board

To oversee IT effectively, the audit committee (or the board, as the case may be), may need access to expertise at its meetings. However, 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.⁷ Members reject the idea that the board should appoint directors who are technology specialists, however. One member said, *"We need diversity on the board and the audit committee ... We need non-financial experts on the audit committee [to provide] breadth and relevant industry experience. We don't need narrow experts, as their shelf life is too short."*

One member pointed out that communication between the CIO and the audit committee can be strained, in part for cultural reasons: *"The culture at many companies is that the IT function is an island; people have great technical expertise but are not good communicators. You need to cut through this engineering-type presentation and ask what is really going on."* However, other members said, in the words of one audit chair, *"If I need someone to interpret what the CIO is saying, we have the wrong CIO."*

Those members who favor the idea of specialists tended to identify people who had gained technical expertise during earlier careers. One member, speaking before the meeting, said the ideal expert is *"selected for their broader aspects. They [are] CIOs who became CEOs."*

The audit committee or board can also consult other sources of expertise:

- **External auditors.** One member said, *"Keep [communication] channels open. It is the best insurance policy you can have."* The external auditor needs to look at the quality of financial controls before signing the financial statements, and audit teams include IT experts who focus on the complexity and risk of applications. One IT auditor estimated that 15–25% of audit hours are IT-related.
- **Internal auditors.** Internal audit is a key source of IT expertise for the audit committee. However, *"Staffing up is a challenge, particularly in IT audit."* Another member agreed: *"It's a sellers' market."*
- **360-degree view.** Several members recommended getting a 360-degree view of IT risks. One audit chair recommended getting perspectives from *"IT auditors, external auditors (who have been all over IT due to Section 404), benchmarking [with peers], vendors, insurance companies (who underwrite certain risks). I wouldn't rely on any one of them [alone]."* One member commented, *"You need both internal audit and external audit, in case one has a reason not to tell you something."*
- **Advisory board.** One member revealed that one company's board is replacing its technology committee with a paid advisory committee of experts to work with management. Board members did not have the required level of expertise to sit on a technology committee, and the board could not find candidates with expertise who could also add value across the whole board agenda. The chair of the new advisory committee will report to the board twice a year. Several members thought this was a

⁶ Tim McCollum, "Everett C. Johnson, Jr., CPA: Bridging the Great Divide," *Internal Auditor*, February 2006, 49. Available to subscribers only.

⁷ 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

useful model that could be implemented in their own companies, and European audit chairs also endorsed this approach at their own meeting.⁸

IT oversight by the audit committee and the board

The board may delegate responsibility for elements of IT oversight – and in some cases complete responsibility for IT oversight – to the audit committee. Generally, however, the board does retain some oversight responsibility.

Role of the audit committee

Existing regulation and legislation offer little guidance on the role of the audit committee in IT oversight. Members report two different approaches to audit committee oversight of IT: the board may delegate oversight of IT governance (including technology risks) to the audit committee, or the audit committee may have responsibility only for technology risks:

- **The audit committee oversees only specific IT risks, often related to financial data.** Several members said their audit committee is mainly interested in financial risk. One member said, *“The audit committee accepts ownership of the controllership of financial data. Every couple of months we review the availability, integrity, and protection of data; both the processes involved and the performance.”*

The fact that IT auditors and others in the internal audit function often report to the audit committee also ties the committee to oversight of IT risks. One member said, *“There are aspects of [IT oversight] that mesh well with the competency of the audit committee, such as the support of internal audit in the field.”* The audit committee may also act on behalf of the board to monitor and review specific IT risks and projects.

- **The audit committee oversees all IT governance, including risks.** In other companies, the audit committee is the lead committee on oversight of the IT function, often by default, because *“it is tough to get anyone [else] to take ownership of it.”* One member commented, *“We want to understand the decision-making process in IT ... We probe for the quality of the process. We don’t second guess whether management was right to engage in a project.”* This audit chair tested whether the right technology was being used by asking, *“Where do you get your ideas from?”*

Role of the board

Members broadly agree with writers of a recent article in the *Harvard Business Review* who said, “There is no one-size-fits-all model for board supervision of a company’s IT operations. The correct IT approach depends on a host of factors, including a company’s history, industry, competitive situation, financial position, and quality of IT management.”⁹

⁸ European Audit Committee Leadership Network: “IT governance,” 7.

⁹ Richard Nolan and F. Warren McFarlan, “Information Technology and the Board of Directors,” *Harvard Business Review* 83 no. 10 (October 2005). Available to subscribers at: [http://harvardbusinessonline.hbsp.harvard.edu/hbrsa/en/hbrsaLogin.jhtml;\\$urlparam\\$kNRXE2ULYRiR52NiWjYH5SF?ID=R0510F&path=arc&pubDate=October2005&_requestid=57873](http://harvardbusinessonline.hbsp.harvard.edu/hbrsa/en/hbrsaLogin.jhtml;$urlparam$kNRXE2ULYRiR52NiWjYH5SF?ID=R0510F&path=arc&pubDate=October2005&_requestid=57873)

Most members agree that the board's responsibility for disclosure and controls requires it to provide a minimum level of oversight. One member said, *"IT impacts data availability and reliability, so we have a responsibility."* Other members said IT deficiencies highlighted by Section 404 compliance also demand board oversight. Members outlined several possible models of board oversight:

- **Board provides regular oversight of IT as a function.** Several members said their boards review IT as a function once or twice a year, receiving a report from the CIO or equivalent. The board is told how IT performs, what the decision-making process is, what the authorization levels and budgets are, and how IT aligns with the business strategy and processes.
- **Board provides regular oversight of IT risks.** Some boards do not oversee IT as a function, but they do oversee IT risks. One audit chair drew a distinction between enterprise-wide IT risks (e.g., business continuity), which the board handles, and IT-related financial risks (e.g., internal controls), which the audit committee handles.
- **Board provides ad hoc oversight of IT as part of another business issue or project.** Some members said the idea of a separate and distinct board discussion of IT strategy does not make sense because technology is integral to the overall business strategy, and any discussions are related directly to general market and product issues. Other members said their boards focused on a particular implementation program during the life of that project.
- **No board oversight of IT; delegation to audit committee.** Some boards reject even the minimum level of oversight suggested earlier. One member said, *"The board views the audit committee as the group to oversee technology. It is not a board role."* The board is kept informed through the regular audit committee report and can ask for a follow-up report from IT if needed.

Several audit chairs felt their boards were pushing management to look at IT more seriously. One member said, *"It is appropriate for the board to ask questions today about what could happen in the next 10 years. In financial services, the focus is on integrity of data, due to the quantity of money moving around. In non-financial companies, there is ... less focus by senior management on these issues."* Another member agreed, saying, *"If management sees IT as a core business process, they will focus on it more."*

Should the board have a separate technology committee?

Corporate Board Member recently reported that "a growing number of boards are setting up special committees to oversee technology ... The Corporate Library, a shareholder watchdog and research firm, looked at more than 2,100 corporations and found 47 whose boards have technology committees."¹⁰ This analysis was conducted in 2005. When The Corporate Library re-analyzed the data in June 2006, the results showed 86 companies with technology committees.¹¹

Several members serve on the boards of companies with technology committees. However, many members are skeptical of the value of a separate technology committee. One said, *"This is not a big enough subject for a dedicated committee."* Another member said the board had decided against creating a technology

¹⁰ Julie Connelly, "More Boards Are Setting Up Technology Committees," *Corporate Board Member*, May-June 2006. Available to subscribers at: http://www.boardmember.com/issues/archive.pl?article_id=12468

¹¹ The Corporate Library conducted its analysis for Tapestry Networks on June 9, 2006, on a database of 2,143 public companies that it follows.

committee: “We don’t have anyone [on the board] with a technology background. When we discussed creating [a] board committee for technology, [that] was one reason we chose not to.”

Examples of technology committee objectives:

- **Oversight of specific IT projects.** One member, whose company set up a technology committee to oversee a major IT investment, said, “It was all about balancing the workload ... These [IT-related risks] come up often, and with a very strong focus. They go to the IT committee. The IT and audit committees have joint sessions now and again to compare notes.”
- **Focus on future technologies.** Another member, who focused on technology as an enabler of the business, said the technology committee “looks more at ... things that we should be doing for business growth.”
- **Oversight of IT governance.** Some companies have given the technology committee responsibility for oversight of the IT function. After considering whether the audit committee should handle IT governance, one audit chair said of the technology committee, “Now we have a place to send IT.”

Conclusion

For members of the Audit Committee Leadership Network in North America, while compliance and controls are key drivers of audit committee oversight of IT risk, they are not the only ones, or even the most important. Other drivers include business continuity and IT security and privacy considerations, especially post 9/11. For the European Audit Committee Leadership Network, a focus on internal controls, whether driven by the need to comply with Sarbanes-Oxley Section 404 or not, was seen as slowly pushing European audit committees toward greater consideration of IT issues – at least as they impact financial reporting. Still, audit committees on both continents face the challenge of agenda overload. For those that cannot devote the time to IT risks and governance, the question remains, “If not us, then who?”

About this document

The Audit Committee Leadership Network is a group of audit committee chairs drawn from leading North American 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 environment.

ViewPoints 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 *ViewPoints* lies in its power to help all constituencies develop their own informed points of view on these important issues.

The views expressed in this document represent those of the Audit Committee Leadership 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.

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