



Information technology governance

Introduction

The North Central Audit Committee Network¹ (NC ACN) met on October 23, 2006 to explore information technology (IT) governance – particularly IT risks and opportunities – and the problems audit committees face in overseeing IT without an IT expert on the board. The network also discussed the sources of expertise upon which audit committees draw to understand IT issues. The members of the network present at the meeting, who sit on the boards of 22 large-, mid-, and small-cap public companies between them, were:

- Jim Boland, Audit Committee Chair, The Goodyear Tire & Rubber Company
- Gordon Harnett, Audit Committee Chair, PolyOne
- Bill Lawrence, Audit Committee Chair, Ferro
- Mike Losh, Audit Committee Chair, TRW Automotive
- Dave McCammon, Audit Committee Chair, Pulte Homes
- John Shuey, Audit Committee Chair, Cooper Tire & Rubber Company
- Paul Smith, Audit Committee Chair, Constellation Brands
- Gary Valade, Audit Committee Chair, Wabtec

Other participants in the meeting included:

- Frank Gori, North Central Area Managing Partner, Audit and Advisory Business Services, Ernst & Young
- Jim Martin, Technology and Security Risk Services Partner, Ernst & Young
- Al Paulus, Senior Client Service Partner, Ernst & Young

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.

¹ The North Central Audit Committee Network (NC ACN) is composed of audit committee chairs drawn from leading companies based in the Lake Erie and Ohio Valley regions of the United States. 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.

VantagePoint is produced by Tapestry Networks to stimulate timely, substantive board discussions about the choices confronting audit committee members, executives, 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, executives, and advisers who become systematically engaged in this dialogue, the more value will be created for all.



Executive summary

IT systems and departments have become integral, indispensable elements in the operations and information flows of efficient and competitively vibrant corporations. It is imperative that mission-critical IT systems operate as intended and without disruption, and that financial reporting information is reliable and secure. Board directors are increasingly – and justifiably – concerned about IT risks and are becoming more involved in IT oversight. The audit committee has been drawn into this key governance arena in part because of its risk oversight responsibilities, including those spelled out in the Sarbanes-Oxley Act, relating to financial reporting and internal controls.

However, audit committees approach the IT arena with caution. NC ACN members acknowledge that few directors possess the specialized knowledge necessary to fully understand IT risks and issues. Members explored the following areas of IT governance:

- **IT risks and opportunities** (*pages 2–5*)

Given their financial risk oversight role, audit committees tend to discuss IT risks more than they discuss the use of IT to secure competitive advantage and seize opportunity. Understanding a company’s *IT environment* and having more regular contact with the chief information officer (CIO) were identified as ways audit committee chairs could gain greater familiarity with IT risks, challenges, and opportunities.²

- **IT oversight: the problem of expertise** (*pages 5–6*)

Network members acknowledged the problem of lack of IT expertise on the audit committee and the board, but they do not think designating a board seat for an IT specialist is the answer, because they believe few such specialists possess the breadth of business experience required of a board member. One member feared a specialist director could become an advocate for IT rather than an impartial overseer. Audit committees that take on IT oversight must often look outside the committee for advice and expertise. IT specialists in internal audit are considered the “*scarcest of scarce resources*” – good to have, but hard to find and keep. Members strongly supported the idea of bringing in outside IT experts (from either the external auditor or an IT specialist firm) who work selectively and in an advisory capacity with the audit committee.

IT risks and opportunities

IT systems, heralded for the benefits they deliver, can also introduce unforeseen risks and vulnerabilities into an organization. The audit committee is more preoccupied with those risks than with IT’s benefits, and members recognize that they generally have less expertise in IT than they do in other business disciplines. Members noted that when an IT issue appears on the audit committee agenda, it usually concerns either the organization’s data security or an operational systems problem (e.g., redundant legacy systems or the risk that

² Questions for the audit committee to ask management about IT-related risks can be found in the appendix on page 7.



a new IT project will not be completed on time). Members admitted that when a major new system is proposed, many board directors and senior executives *“don’t know what they are talking about.”*

IT applications are greatly integrated in financial reporting processes from initiating, authorizing, recording, processing, and reporting transactions. Therefore, understanding a company’s IT environment is necessary for members to adequately oversee IT-related risks.

Key elements to understanding the IT environment

Element	Consideration
Number of applications relevant to financial reporting	Few (< 5), moderate (5 – 20), many (> 20), breakdown by business location
Nature of applications	Complex or simple, unique or common, customized or not customized, developed in-house , purchased or age of application
Nature of IT processes	Centralized or decentralized; common or unique, formalized or ad hoc
Nature of people	Level of experience, training, and turnover
Datacenter locations	Domestic or foreign, in-house or outsourced
Nature of planned changes (e.g. over the next 12-24 months)	Impact on business and IT environment (people, process, technology)

Not understanding or ignoring a company’s IT environment can prove hazardous not only to a company’s bottom line, but ultimately to its survival. One member described the losses a company incurred when it faced IT system implementation challenges: *“Once [a bad IT system] is out of the package, it’s a disaster. One company lost tens of millions of dollars in sales ... [A failed IT system] could put a company out of business.”* The member said people at that company were working 15 hours a day for six months to remediate the damage. In light of that sobering reality, members agreed that audit chairs should take a closer look at what is happening within their IT departments and endeavor to meet with the CIO on a more regular basis. Only half of members said their CIOs are invited to audit committee meetings on a regular basis. At a minimum, as one member said, *“I would like to see the CIO come to a board meeting once a year.”*

Greater engagement with the CIO will make audit committees more familiar with the IT environment and more alert to potentially costly mistakes. And there are other lasting benefits from direct interaction between the audit committee and the CIO. First, issues can be addressed immediately, and the audit committee can determine what becomes the committee’s responsibility (primarily compliance, control, and operational risks)



and what is more strategic and requires full board attention. One member described how knowing his IT environment had brought clear benefits: a review of his company’s IT disaster recovery plan revealed vulnerabilities; the member then instituted a six-month review of the plan, with specific remediation objectives identified.

In terms of fundamental attitude, understanding the organization’s IT landscape requires a break from the historical bias that regarded IT as a “back burner” function, of little concern to the audit committee. The appendix on page 7 offers questions that audit chairs can ask their CIOs to help them better assess their IT vulnerabilities and avoid dedicating time to low-value IT “fringe” issues.

IT risk: an audit committee concern

With IT systems managing such critical tasks as accurate and timely financial reporting and storing of customer databases and proprietary company information, organizations cannot afford to settle for lax controls or disruptions to their technology platforms. Careful attention must be given to IT system risks. One member noted that while large IT capital expenditures often require oversight by the full board, any problems with IT implementation “*falls naturally to the audit committee.*” Members observed that companies in regulated industry sectors such as financial services and insurance have deeper experience in managing their IT risks.

The most prevalent and immediate concern for members is the question of internal security and up-to-date access controls. One member commented, “*IT people move around a lot [between companies], and there is bad coordination between the human resources and IT departments [in terminating former employees’ systems access].*”

Finally, audit chairs must be prepared for a major business disruption. One member commented, “*If your IT system goes down, you are in deep trouble.*” The terrorist attacks of September 11, 2001 and the devastation of Hurricane Katrina have brought the issue of business continuity planning, including the use of outside vendors, into sharp focus. A member of another audit network commented, “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.”

The following five risks were identified as key challenges for audit committees:

Five key IT-related risks and challenges

- 1. Compliance and controls – can we rely on the integrity of information?
- 2. Integration and centralization of IT systems – can we be efficient and cost effective?
- 3. Security and privacy – can we keep the bad guys out?
- 4. Project delivery – can we get value for our IT investment?
- 5. Comprehensive strategy – can we use IT for competitive advantage?



Opportunities and benefits

Although audit chairs worry about IT risks, there are opportunities and benefits associated with IT in the areas of compliance and business growth. 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 For all the pain associated with the introduction of Sarbanes–Oxley and Section 404, the requirements imposed by the legislation actually motivated many IT departments to streamline and better secure firm-wide IT systems.

Another important outcome of Section 404 is that as companies centralize and standardize their IT systems, opportunities are created to centralize and standardize business processes. A member agreed saying, “*centralization and standardization are key drivers for many company’s globalization strategies.*”

As for growth-related opportunities, although audit chairs of companies in traditional manufacturing industries often view their IT systems as playing a support role rather than as drivers of competitive advantage, many members felt the effective application of IT could contribute to the growth of the business.

One member described a tool that enables customers to “*tap in and find out where his or her order is,*” noting that this simple customer service feature can lead to customer loyalty and retention. Another member commented that he was surprised by “*how little we talk about IT creating competitive advantage.*” Every company’s comprehensive strategy should include thoughts on ways to mitigate the risk of having its IT systems become obsolete, especially in the context of a competitor’s potentially moving to a more advanced technology platform. Members decided that this is an issue for the full board but believed that the audit committee could serve as a catalyst to get the issue on the agenda.

IT oversight: the problem of expertise

Traditionally, audit chairs receive scant guidance on how they should oversee IT. One reason may be the lack of qualified IT specialists elected to the board. Only one of the eight members in the meeting felt he had deep IT experience. Nevertheless, members do not believe that companies should recruit IT specialists to their boards. One member said, “*You don’t want to give up a [board seat] for this [IT specialist]. The half-life of IT knowledge is too short, so it’s not worth it.*” Another member was more explicit: “*Many CIOs have too narrow an experience to sit on most big company boards.*” However, one member offered a countervailing view, observing that “*some CIOs have a great handle on the business ... especially knowledge that cuts across the entire business.*”

While some audit committees have the expertise necessary to assess and oversee the remediation of risks associated with IT systems, many do not. Therefore, they often look for assistance from other sources:

- **Internal audit.** A number of members said they had hired IT specialists for internal audit but acknowledged that these specialists are “*the scarcest of scarce resources.*” One member’s company hired an internal audit IT specialist outside the normal salary band, while another shared that his internal audit

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.



group has two IT specialists “*who do nothing but IT-related internal audits around the world.*”

However, those specialists may be hard to keep in a tight market. One member cautioned, “*If you have an international company, [your IT internal audit specialists] are gone in six months.*”

- **External audit.** Audit committee chairs can discuss IT matters with the accounting firm’s IT experts on audit teams to ensure that members understand the IT environment and the related risks, controls and control gaps that may exist. Three good reasons for close cooperation with external audit are (1) the external auditor knows the company, (2) the external auditor knows how IT impacts controls and other risk areas, and (3) the external auditor has the resources and ability to provide current perspective on IT risks, challenges and opportunities.
- **Third-party IT and accounting firms.** Some companies will hire third-party IT firms to assess their IT systems and security measures. The process can include everything from mock attacks on the company’s IT system to a road map for centralizing disparate applications and capabilities.

Regular testing of IT security by outside sources can help companies address any deficiencies promptly. Once testing is complete, the results are reported back to the audit committee. The same holds true if internal audit uncovers possible misfeasance or control improprieties. One member said that if a problem is suspected, “*You peel back the [IT] system, and you find issues that could be material.*”

Since oversight of IT remains for the most part undefined and rather ad hoc, outside assistance is often an effective way to ensure that a company’s IT risks and controls are being examined thoroughly.

Conclusion

North Central Audit Committee Network members left the meeting convinced that they need to give IT a more prominent place on their audit committee agendas. The risks and opportunities represented by IT are simply too great to leave unattended. However, in many cases, the roles of the full board and the audit committee need to be clarified.

Members also saw the need to build deeper relationships between the audit committee and the CIO, so there is a regular channel of communication regarding the IT system’s risk, challenges and opportunities. The more attuned audit committee members become to their IT environment, whether through regular committee interaction with the CIO or through the use of other resources, the better positioned they will be to mitigate risks and make informed decisions.

The views expressed in this document represent those of the North Central 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.

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.



Appendix: what the audit committee should ask the CIO⁴

Internal controls

- Once system controls are developed, how do you ensure they stay in place? What events could cause IT controls to fall out of compliance?
- How can IT help make Section 404 compliance more sustainable?

General IT controls: access

- What have you done to ensure segregation of duties? How do you ensure that access rights change when people change jobs?
- How many people have sufficient access to significantly disrupt the company's network? What are the limits on their access?
- How do you ensure that mission-critical and/or sensitive information is protected?

General IT controls: program development and change

- How confident are you that all software is documented and meets quality standards (and that backdoor entry points created during application development are closed)?

Crisis prevention and management

- What framework does IT use to assess actual risks, risk awareness, and risk prevention?
- How long could the company's systems be down in a crisis event before significant damage to the company was done?

Outsourcing

- Are all outsourced operations SAS 70 compliant?

Value creation

- How does IT contribute to shareholder value?
- What metrics do you use to evaluate your work? What other metrics should be used?

⁴ Ibid.