



## Information technology governance

### Introduction

The Mid-Atlantic Audit Committee Leadership Network<sup>1</sup> (MA ACN) met on January 11, 2007, to explore information technology (IT) governance, IT risks and opportunities, and the role of the board and the audit committee in IT oversight. The network discussed ways to oversee the IT function effectively at the level of the full board and the audit committee; it also discussed sources of expertise upon which both the board and audit committee can draw to understand IT issues.

The members of the network present at the meeting, who sit on the boards of 19 large, mid-, and small-cap public companies between them, were:

- Jim Brady, Audit Committee Chair, Constellation Energy Group
- Bob Grafton, Audit Committee Chair, CarMax
- Charlie Hopkins, Audit Committee Chair, Charming Shoppes
- Mike Ressler, Audit Committee Chair, Magellan Health Services
- John Schwieters, Audit Committee Chair, Smithfield Foods
- Paul Shapiro, Audit Committee Chair, Toll Brothers
- Larry Small, Audit Committee Chair, Marriott International

Other participants in this meeting included:

- Mark Bartlett, Managing Partner, Baltimore office, Ernst & Young
- Mike Herrinton, Mid-Atlantic Area Technology & Security Risk Services Leader, Ernst & Young
- Rich Jeanneret, Mid-Atlantic Area Managing Partner, Assurance and Advisory Business Services, 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.

---

<sup>1</sup> The Mid-Atlantic Audit Committee Network is composed of audit committee chairs drawn from leading companies based in the Mid-Atlantic region 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 audit environment.

*VantagePoint* is a synthesis of some key issues arising from a facilitated discussion among members of the Mid-Atlantic Audit Committee Network. It is intended 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

In recent years, companies have become increasingly reliant on technology for the efficient and accurate flow of information. Because IT systems are central to many functions, including marketing, operations, and financial reporting, board directors are increasingly concerned about IT risks and are becoming more involved in IT oversight.

MA ACN members acknowledged that few board directors have current, specialized IT expertise. As a result, some audit committee members are less comfortable with IT oversight than they are with other areas of responsibility. Members shared several key points:

- **IT oversight is increasingly important for audit committees and boards** (page 2)

Although directors have traditionally provided little oversight of the IT function, it is an increasingly important priority for boards and audit committees. The level of oversight required and how responsibilities are divided between the audit committee and the full board depends largely on the magnitude of the IT investment and the importance of IT as a strategic enabler.

- **Audit committees benefit from interactions with IT leaders and technical advisers** (page 3)

Members say their audit committees are meeting more frequently with the chief information officer (CIO) and other IT leaders than they did in the past. Most members report at least an annual briefing; some CIOs attend every board and audit committee meeting. A CIO who rises beyond the role of technical expert to that of a business partner for other senior executives is especially valued. Members also rely on technical expertise provided by internal or external auditors and IT consultants.

- **IT oversight is an important aspect of enterprise-wide risk management** (page 5)

Because IT systems reach into all aspects of a business, IT risks cannot be isolated from other operational, strategic, or reputational risks. Consequently, IT risk oversight should be viewed as part of the board's overall risk oversight activity. The trend toward centralized IT systems has helped to decrease overall enterprise-wide risks by decreasing the number of systems that need to be monitored, protected, and backed up.

## IT oversight is increasingly important for audit committees and boards

Historically, board members have provided relatively little oversight of IT. As one network member stated, *"If I look at all the boards I've ever been involved with, I don't think it can be stated factually that the board oversees IT."* Members expressed some lingering concern about the challenge of providing such oversight. One member noted, *"[IT] is the area [with which] top management is least comfortable. The board's not comfortable, nobody's comfortable, but everybody says how important it is."*

For many companies, Section 404 highlighted IT control vulnerabilities, and members are increasingly aware of the importance of board-level IT oversight. However, they point out that there is no "one size fits all" approach to IT oversight. Factors that impact the nature and level of the board's oversight include the company's strategic dependence on IT, the level of enterprise risk associated with the IT decisions, and the scale of the IT investment.



### Five key IT-related risks and opportunities for boards to consider

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

Because IT systems support companies' financial reporting and internal control processes, members agreed that the audit committee must be involved in some aspects of IT oversight. The question that concerned members most was where to draw the line between the audit committee's responsibilities and those of the full board.

- **Audit committee responsibility.** Members generally agreed that the audit committee should focus on the accuracy and integrity of financial information delivered through IT systems, the effectiveness of internal controls, and risks associated with IT. One member expressed concern about overloading the audit committee, but stressed the importance of the audit committee's role in IT oversight, saying, *"I get nervous when we say [IT] should be in the audit committee, but it's so central to what we do that we have to have a distinct role."*
- **Full board responsibility.** Reflecting on the prevalence of IT systems in most corporations, one member said, *"The business is not just using IT to support finance. It's [all] handled by the same IT department ... Do you just discuss what they are doing on finance at the audit committee? It's so mixed; we just do it at the board."* Another member agreed: *"The full board ought to be privy to where IT is every year. It can't be buried in the audit committee."* Network members advised that the full board handle IT oversight when the technology is a fundamental source of competitive advantage, when IT is closely aligned with strategic initiatives, or when an IT project represents a significant capital expenditure. However, one member said the board only needs to be involved when a system implementation involves significant risk to the enterprise: *"If a company wants to buy an expensive system, it's nice to know, but I don't think it's critical ... I can't imagine board members having the [necessary technical] knowledge to judge if a system is good or not."*

### Audit committees benefit from interactions with IT leaders and technical advisers

Members acknowledge that few directors are appointed to boards on the basis of deep IT experience. However, members believe that even if directors lack a technical foundation, they can still provide an appropriate level of oversight by expanding and enhancing relationships with IT leaders and drawing on sources of expertise from inside and outside the company.

One network member said, *"We rely on internal and external audit to give us a reading on where we stand from an IT perspective."* However, several members noted that IT experts in internal audit have become a *"hot commodity,"* making it difficult to recruit and retain qualified staff. Consequently, several network



members said they rely less on internal audit and are more likely to turn to their external auditor, or another accounting or IT services firm, for this expertise.

### Improving IT governance

Members mentioned several other ways their boards and audit committees have improved the quality of IT governance:

- **By developing a relationship with the IT organization.** Many audit committees have started to develop a deeper relationship with the CIO and the IT function. *“I see the CIO [as being similar to] the head of internal audit. I want a relationship with him, to be comfortable [with him], and I want the audit committee to know him.”* Members’ levels of interaction with the CIO varied based on the individual in that role and the nature of the business. Not surprisingly, interactions between the audit committee and senior IT leaders tend to be deeper and more frequent in companies that rely heavily on IT as a source of competitive advantage. Two members reported that the CIO attends virtually every board and audit committee meeting.
- **By insisting on regular presentations from IT executives.** Members point out that even periodic board presentations by IT executives will *“get the attention of management.”* One member said, *“I don’t think any of us [fully] realize the importance of making management present to the audit committee ... The discipline is pretty powerful.”* Another said, *“The CEO and CIO say it is helpful that people have to give a presentation every year ... I don’t understand all of it, but there is value in making them report clearly.”* Some members caution that annual board presentations from the CIO may not be sufficiently frequent; however, there was consensus that even limited interaction between the audit committee and the IT organization can provide disproportionate benefits, in part by setting an appropriate tone and focus.
- **By understanding the IT environment.** Board members should understand the company’s overall technology strategy, including the degree of IT centralization, and ensure the organization has clear, consistent policies and procedures on an enterprise-wide basis. Boards should have a basic awareness of major system upgrades, the stability of legacy systems, and vendor support for both new and legacy systems. Audit committees should pay particular attention to applications that support financial processes, and to the underlying infrastructure that supports these applications.
- **By asking the right questions.** Asking the right questions can help cut through technical jargon and garner useful information. One member said, *“You can only know so much [about technology], but ‘Columbo-esque’ questions are good. What are the projects you’ve considered, but decided to defer to future years? You can get a sense of the temperature in the company.”* Members point out that it can be difficult for directors to ask the right questions when they lack relevant expertise; in such cases, members advocate drawing upon available sources of expertise for support in developing such questions (see the Appendix, page 7).



## The attributes of effective CIOs

Members agree that the CIO should be more than simply a technical expert. Increasingly, CIOs are expected to oversee complex global organizations, manage significant budgets, and participate in important strategic decision making. In some cases, the CIO is one of the top five named corporate officers. While many qualities differentiate a great CIO from one who is merely good, members identified several key attributes (see box below).

### Audit chairs believe an excellent CIO must have...

- The ability to communicate effectively with non-technical senior executives and board members
- Good executive leadership skills, along with technical expertise
- Effective political and diplomatic skills
- An interest and appreciation for the business that surpasses their love of technology
- An ability to develop bench strength within the IT organization to ensure leadership succession
- Broad experience in different areas of the business, to build internal credibility as a leader

## IT oversight is an important aspect of enterprise-wide risk management

According to leading CIOs interviewed for *InSights* two years ago, “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.”<sup>2</sup> Members agreed that despite what has been seen as excessive cost and pain associated with Section 404 compliance, the process had led to greater awareness of the risks and weaknesses in companies’ IT systems and forced management to focus on mitigating those risks. One member noted, “*Three-quarters of the glitches, exceptions, and issues [in Section 404 compliance] were associated with IT, not other accounting or internal control functions.*”

Given the audit committee’s responsibility for financial reporting controls and risk management, members recommend that it not treat IT risks in isolation, but instead consider the impact of IT risks as part of the broader enterprise-wide risk management effort. As one member pointed out, “*The whole business may be resident*” in IT systems, and that should be factored into the committee’s approach to IT risk oversight.<sup>3</sup>

In particular, members said audit committees should pay close attention to the following IT risks:

- **Security and access controls.** Members are deeply concerned about IT security and access controls, both internal and external. They expressed particular concern about the reputational risk associated with an internal breach, which sends “*the wrong message*” about the company’s controls. Most members agreed that Section 404 compliance has helped focus attention on vulnerabilities in this area.

<sup>2</sup> 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](http://www.tapestrynetworks.com/documents/Tapestry_EY_ACLN_Feb05_InSights.pdf).

<sup>3</sup> Members also noted the benefits that had come from integrating IT systems, centralizing processes, and improving customer-facing functions, but most did not see those elements as falling within the purview of the audit committee’s oversight responsibility.



- **Privacy.** Businesses that are in possession of large amounts of customer data are extremely anxious to safeguard it. According to one member, *“We’re most concerned about privacy. We are paranoid about controls over that.”*
- **Implementation.** One meeting participant cautioned that large-scale enterprise system implementations often constitute a significant operational risk and asserted that these projects generally do not receive sufficient board attention. In some cases, boards may need to increase their oversight of such projects to ensure appropriate rigor is applied to timetables, operational integrity, and budgets.

Members also noted the benefit of centralized and integrated processes in Section 404 compliance. One member confided that *“404 would have been four times the nightmare”* if the company’s back-office systems had not been centralized. Most members agreed that the trend toward centralized IT systems has helped to reduce enterprise-wide risks, including operational and compliance risk. Centralized IT systems require fewer, better IT professionals to manage a single, centralized system, require less backup and redundancy, and decrease compliance costs.

## Conclusion

Mid-Atlantic Audit Committee Network members agreed that the risks and opportunities associated with IT require more oversight from the board and the audit committee. They acknowledged the benefits that IT systems can provide in mitigating risk and building competitive advantage, but they noted that few boards spend significant time discussing those opportunities at either the audit committee or full board level.

In some cases, audit committees may need to expand their scope of responsibility to include specific IT issues. In other cases, IT oversight responsibilities may fall to the full board. Either way, the audit committee chair can serve as a catalyst, working with board colleagues to shape the agenda in order to ensure that relevant issues are discussed, that key risks are mitigated, and that management has a plan to align IT activities with strategic and operational objectives.

*The views expressed in this document represent those of the Mid-Atlantic 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: Questions the audit committee should ask the CIO<sup>4</sup>**

### **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?

---

<sup>4</sup> Ernst & Young and Tapestry Networks, "The CIO's perspective," 9.