



AUDIT COMMITTEE INSTITUTE

# IT Governance – Where Does the Audit Committee Fit?

KPMG IN CANADA

Reprinted from *Canadian Audit Committee Update*, Issue 2007-02

The way a company leverages its information technology is an important factor in meeting its business objectives. However, debate continues as to what IT governance is and how it is achieved.

The way a company leverages its information technology is an important factor in meeting its business objectives. However, debate continues as to what IT governance is and how it is achieved. The audit committee has a keen interest in IT governance since it oversees many areas that are often highly dependent on the quality of information processed by computer systems, such as financial reporting and compliance with legal and regulatory requirements.

*Some audit committees are focusing on information being managed and not on the managing technology.*

What exactly is the audit committee's role in overseeing the company's information technology? This can be a difficult question to answer. Any IT discussion can quickly get bogged down in technical jargon, with the result that it can become unclear who is responsible for oversight of technology-related risks. It should be no surprise then, that in many organizations, audit committees are questioning how well IT is governed, and, indeed, who should have responsibility for its oversight. To clarify and manage their responsibility for oversight of IT, some audit committees focus on the information being managed, not the technology being used to manage it.

Many items on the audit committee agenda involve technology. The impact of IT is pervasive, from financial and regulatory reporting, internal control certification, business continuity, and IFRS conversion, to the myriad of laws governing the protection of personal data. Although these are critical business issues, the information needs of a company extend much further than the ambit of the audit committee. For example, the same customer transaction information feeding financial reporting may be critical to the company's sales and marketing activities. How an organization manages its information, not to mention how it manages the often substantial costs of its IT investment, is often pivotal to its competitiveness and ultimate success.

## IT governance – a shared concern

IT governance can be thought of as how a company achieves its business objectives through the use of technology. How narrow or how wide IT governance is defined varies from company to company. The common theme is “How can we ensure we get the right information to be used in the right way, at the right time?”

A number of governance frameworks point to a holistic definition, whereby the value of IT to a company can be measured and monitored in several different areas simultaneously, such as:

- compliance with applicable laws, including financial reporting
- control of IT costs
- project delivery timeliness
- risk management
- alignment of IT with operational objectives.

*Oversight of IT rests with more than one group.*

In practice, these IT areas affect different parts of an organization and frequently the responsibility for their oversight does not rest with only one group. There is often a dual ownership of the systems by users and IT. The IT department “manages the machines” (i.e., purchases, implements, and maintains the tools used that contain, process, protect, and report the information). After all, if a computer crashes—it’s the IT department that fixes it. However, many chief information officers are quick to point out that too often the assumption is made that control of the technology is control of the information. The ownership for the information being entered into the systems, the controls applied around the systems, and the use of the information rests with users such as finance, sales, and others who play a critical supporting role.

If the basis of good governance is accountability and responsibility, then who is in the best position to provide overall oversight of an area that spans such different areas of the organization? Ultimate oversight responsibility should lie with the board of directors. In some organizations, this may be further assigned to the audit committee since a substantial part of IT is often devoted to managing the processes and risks that affect financial reporting.

But is it possible to be responsible for only a part of the oversight of IT governance? What about all the other impacts of IT on an organization, such as cost control, legal compliance, and customer satisfaction? They may not directly impact financial reporting or regulatory matters, but can be affected by the overall quality of how IT is governed. Who oversees that part of IT governance impacting these other areas? Is the audit committee left with responsibility by default? Do audit committee members have the time and the expertise?

*Audit committee member survey sheds light on audit committee oversight of IT.*

According to the 2007 survey of audit committee members by KPMG's Audit Committee Institute and the Institute of Corporate Directors, there is variation in practice. When asked about the specific areas of IT for which their audit committee holds primary responsibility for oversight, almost 60 percent of respondents indicated IT compliance and controls, and slightly less than half identified business continuity and information security/privacy. One in five indicated none of these areas. Of course, an audit committee's role can depend on the size and complexity of the organization. There can also be dissatisfaction with the oversight of IT. Almost one-third of survey respondents indicated that the board's oversight of IT risks "needs improvement" with over half indicating they are only "somewhat satisfied." Audit committees may be ill at ease with their role in an area that has such far-reaching implications for the success of the organization. How does the audit committee achieve its mandate without overstepping their bounds? Some practices are providing useful insights.

*IT oversight is often a shared responsibility.*

### **Clarify responsibilities at the board level**

The board should ensure that IT oversight is appropriately allocated—it is usually not appropriate to mandate oversight of all aspects of IT governance to the audit committee. For example, when a major systems event occurs, such as the development and implementation of a new computer system, oversight that focuses on only financial reporting and regulatory compliance may meet the audit committee mandate, but will not provide sufficient focus on the mission-critical objectives of other large parts of the organization affected by the system changes.

Clarifying the audit committee's role should be a priority. Some companies create a technology subcommittee of the board to oversee the management of the broader IT components in conjunction with the audit committee. Other companies use internal auditors or external consultants to provide specialized oversight. The key is to make sure someone has an oversight role for all major IT components.

*Clear communication is essential to good governance.*

### **Bridge the communication gap**

Clear communication of IT issues can be essential to good governance. It is often seen as a challenge for the technically savvy IT department to clearly communicate to the operational and financial reporting groups. As more complex technologies become commonplace, understanding the rationale for major IT-related capital expenditures has become more difficult for the non-specialist.

If a technology issue cannot be expressed in simple terms, this may be a red flag. Perhaps an IT decision may not be clearly aligned with overall strategic business objectives. Management should be challenged to focus on the implications of changes in how information is managed by the organization, and not on the tools and technology underlying it. It is important to ensure someone has a sufficient knowledge of the technology issues and the business issues to clearly describe each to the audit committee. In some companies, this might be the CFO, the CIO, a special technology committee, or sometimes a third-party consultant.

### **Focus on important matters**

*Focus on strategic IT matters.*

It is important to focus on specific IT items affecting the audit committee agenda, although it may be difficult to put boundaries on the depth of any technology-related discussion. For example, some companies recently toiled laboriously to demonstrate the effectiveness of the systems supporting financial reporting as part of their internal control certification projects. These projects tended to be so widely scoped that it was difficult to see the real impact on financial reporting of much of the effort. When it becomes obvious that not every aspect of IT needs to be included to support internal control certifications, it is possible to simplify the process.

In its oversight role, the audit committee should focus its attention on strategic IT matters. This can be done by asking:

- What are the key IT-related issues affecting financial reporting, regulatory compliance, and risk management processes, and are they receiving enough attention?
- What are the organization's specific strategies to manage these issues?
- Is success in managing these issues clearly measured and monitored?

*Do not be afraid to ask questions.*

If the audit committee should be educated about a particular aspect of IT in order to be able to ask the right question, then take the time to do this—but do not let the technology take centre stage. Most importantly, do not accept vague or unclear answers—experience shows that, with some perseverance, most IT issues can be expressed in relatively simple terms.

The risks involved in managing IT can extend throughout the company, beyond just financial and regulatory reporting. Audit committees are becoming more and more involved in overseeing IT governance—but sometimes by default. This is challenging their abilities to keep up with the ever-expanding complexity and the increasingly pervasive impact of IT on the organization. With increased focus on this important area, the audit committee can help ensure it assumes the right oversight role for IT governance.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG and the KPMG logo are registered trademarks of KPMG International, a Swiss cooperative.  
© 2007 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved. 3563