CPAB exchange

March 2016

Audit Committee Oversight of IT Risk

The Issue

Technology and information systems are an essential part of an organization's strategy and operations, enabling innovation and efficiencies across business processes.

However, the growing reliance on technology and the pace of technological change also creates a higher degree of risk and vulnerability in areas such as security, privacy, disaster recovery, governance and more.

The Canadian Public Accountability Board (CPAB) has heard from audit committees that IT risk is a growing priority for boards and audit committees, yet they often feel ill-equipped to perform their oversight role in this area. Understanding the risks of the organization and asking the right questions of external auditors, internal auditors and management can help audit committees manage its IT risks and protect its information assets more effectively.

Top IT Challenges for Audit Committees

Common IT-related business issues where risks can arise and that audit committees often express concern about include IT security and privacy, systems implementation or conversion, business continuity and disaster recovery and third-party arrangements or outsourcing.

Audit committees cite the pace of technology change (emerging technologies, mobile, social media, data analytics and cloud computing) and cyber security (data protection and intellectual property) as the IT risks that pose the greatest challenges for their organization today.[1]

IT Risk Management Oversight

Traditionally, the role of the audit committee has been primarily focused on financial reporting and the related internal control processes. However, many audit committees now have a broader mandate that includes oversight of the organization's enterprise risk systems and processes, including risks ranging from strategic and operational to environmental and compliance risk. While some boards may have a separate risk committee, in Canada this is primarily limited to large financial institutions. In the absence of a separate risk committee the responsibility of risk management oversight is often delegated to the audit committee. That's why it's important for the audit committee to have a solid understanding of the risks across the organization and related risk management processes.

Many areas of IT risk have become enterprise-wide risk management issues that should be addressed strategically and across multiple functions, instead of as technical issues to be addressed only by the IT department. Where the audit committee is responsible for the oversight of the organization's enterprise risk management framework, it should ensure management has considered the appropriate IT risks as part of the enterprise risk management framework and that risk mitigation and response plans have been developed.

[1] KPMG 2015 Global Audit Committee Survey

Managing Specific IT Risks

Management has responsibility for identifying, assessing, controlling and mitigating IT risk on a day-to-day basis. Once the IT risks of the organization are known and the processes and controls management has in place are understood, the audit committee may choose to seek independent perspectives or assurance over if and how those risks have been mitigated by management. This could be obtained from the external auditor, the internal auditor or from other external specialists. It is important for the audit committee to have conversations with all parties to understand the scope of their responsibilities and their capabilities.

The External Auditor

The external auditor is required to obtain an understanding of the IT control environment and how IT systems are used to support the financial reporting process. If a control-reliance approach is taken, the external auditor would examine the design and operating effectiveness of general IT controls (GITCs) as it relates to the IT systems that support financial reporting, typically focusing on access and changes to those systems[2]. However, many of the areas of IT risk that are of growing concern to audit committees may not be seen to directly create a risk of material misstatement, putting them outside the realm of financial reporting, at least until a significant event occurs.

The Internal Auditor

Where a company has an internal audit function, the mandate may cover operational areas and key risks of the organization, including examining a broader scope of IT risks and systems which often extends beyond financial reporting. The audit committee should review the internal audit plan for the year and ensure that it is aligned with the overall enterprise risk management framework and discuss the areas of risk that should be addressed through their audits.

Cyber Security and the External Audit

The ongoing occurrence of high-profile security breaches continues to keep the topic of cyber security top-of-mind for most boards and audit committees. As part of the financial statement audit, the external auditor is primarily focused on the risk of unauthorized access or changes to those systems closest to the application that supports the financial reporting process, which is the application itself and its supporting database and operating system. However, the risk of a cyber incident is typically greatest around the external perimeter and internal network layers, currently beyond the scope of the audit as it is further removed from the application data and therefore less likely to pose a significant risk of misstatement.

Also, as the external audit focuses on those systems that could impact financial reporting, there could be other non-financial systems within a company that are critical to ongoing operations and vulnerable to attack. It is important for audit committees to understand what their external auditor is and is not examining when it comes to cyber security.

Where To Look For Help

After identifying specific IT risks and considering the risks that are in the scope of the external audit or are reviewed by the internal auditor, the audit committee should identify the areas where additional assurance is required. The audit committee may look to a number of different parties to assist including their external auditor, internal auditor and other external specialists. In doing so, the audit committee may consider the following:

- Many of the larger public accounting firms have resources that specialize in areas of IT risk and can provide assistance beyond their role as the external auditor. Where the external auditor is engaged, the independence of the auditor must be considered. However, in most cases, the external auditor can provide services that extend beyond the financial statement audit without an independence violation if they are not responsible for the design or implementation of the system of internal controls. Management and the audit committee should review independence requirements before engaging the external auditor for additional services.
- Because of factors such as independence restrictions of the external auditor or limited resources and/or skills within the internal audit department, the audit committee may need to consider engaging other external specialists to assess areas of IT risk in the organization.

[2] In situations where reliance is placed on IT-enabled or IT-dependent controls

CPAB eXchange

Questions for Audit Committees

Audit committees should take a proactive approach to understanding key IT risks and how they are addressed. This includes holding management accountable for the identification and mitigation of IT risks, understanding what risks the external and internal auditors are assessing and areas where a gap exists and other external specialists may be able to assist. Below is a list of questions for audit committees to consider:

1. Who is responsible for the oversight of IT risk on the board? If this has been assigned to the audit committee, does it have sufficient information and expertise to perform this role?
2. Does the organization have an enterprise risk management framework and does it consider IT risk?
3. Do the board and audit committee agree that management has identified and mitigated the critical IT risks?
4. What applications and supporting systems has the external auditor determined to be in scope of the financial statement audit?
5. What audit procedures have been performed by the external auditors to address IT risk?
6. Did the external auditor identify any deficiencies in IT? If so, where? How have these been addressed? What is the impact to the company?
7. Did the external auditor identify any other areas of potential vulnerability that may not have a direct impact on financial reporting?
8. Is the internal audit plan aligned with the enterprise risk management framework?
9. Does the internal audit department have the skills, resources and expertise to execute on an audit plan that addresses the critical areas of IT risk within the organization?
10. Does the combined scope of the external auditor and the internal auditor provide an adequate level of assurance on the critical IT risks?

Learn More

Visit us at www.cpab-ccrc.ca and join our mailing list. Follow us on Twitter — @CPAB-CCRC

www.cpab-ccrc.ca / Email: info@cpab-ccrc.ca

CPAB CCRC