Board Perspectives: Risk Oversight

Oversight of IT Risk Management

Issue 53

Nowadays it's a bit trite to observe that technology is evolving rapidly and transforming the way people live, interact, work and play. Deployment of technology to reduce costs, improve business processes and increasingly drive revenue expansion is altering the way companies operate. Increasingly sophisticated user demands coupled with cloud computing, social networking, mobile technologies and other enabling trends are driving disruptive, transformational change in the technological landscape itself.

Key Considerations

How does this changing environment impact board risk oversight? Limiting risk oversight to evaluating individual technology projects as part of approving the capital budget and considering IT risks on an ad hoc, reactive basis is insufficient and simply too narrow a focus. Following are 10 suggestions for boards to consider as they enhance their risk oversight as it relates to IT matters:

1. **Organize for IT risk oversight:** Many boards designate the audit committee as the key oversight body for IT. However, the audit committee's focus is often limited to financial reporting and the related controls. One option is to evaluate strategic IT issues as part of a separate strategy committee or the finance committee, mirroring how the board oversees strategy planning and execution. Depending on the importance of technology as a driver of the overall corporate strategy, a separate technology committee may be warranted. If there is a separate risk committee, it may also be an option. The point is the audit committee should not be viewed as the default choice.
2. **Understand how technology fits within the business model:** IT risk oversight requires some education for most boards. For organizations where technology is a tool for building connections with strategic suppliers, channel partners, customers and outsourcing providers, directors need to understand how IT is integrated with the business. They must look to the CEO, CIO and chief strategy officer to help them acquire this "big picture" view.
3. **Begin with the right questions:** There are three general questions that boards should ask with respect to risk oversight: What are our risks, how are we managing them, and how do we know? These questions apply to IT and often require independent clarification and assessment to be effective. The key to thinking about IT is its disruptive, game changing potential. No organization wants to be on the wrong side of a change in the fundamentals underlying an industry.
4. **View IT as a business:** The CIO organization manages the business of IT. Like any other business, it has customers and suppliers and must ensure the organization maximizes return on information systems investments while at the same time minimizing risk. It must align the IT strategy

with the needs of the organization; establish IT governance, risk management and compliance; and manage IT processes efficiently and effectively. While business alignment is a perennial top management priority for CIOs, it remains elusive for several reasons. For example, many organizations fail to communicate goals, strategies and key success factors clearly; IT personnel may not understand the business sufficiently; or IT efforts are overly fragmented from pursuing too many priorities. Whatever the contributing factors, the board's oversight should ensure there is sufficient emphasis by executive management on securing successful alignment of IT strategy with business needs.

5. **Take an integrated comprehensive view:** While security and privacy breakdowns and service interruptions get the headlines, IT risk includes other important risks warranting the board's attention. IT risk is both a component of many business risks and an area of specific risks that should be evaluated. The virtual organization and the cloud are spreading responsibility for IT infrastructure across multiple independent entities operating at different locations across the globe. Rather than make IT an appendage of the board risk oversight agenda, the oversight process should integrate IT risks into the oversight of strategic, operational, financial and compliance risks. For example, strategic and financial risks include technological innovation, resource allocation and project management risks. Operational and compliance risks include such internal process risks as integrity and relevance of critical information, security and privacy, availability of IT resources, efficient allocation of costs to IT services, and infrastructure risks.
6. **Watch out for the effects of change on IT infrastructure:** Whether an organization is expanding, contracting or maintaining a steady market position, it is important for directors to recognize that in today's IT landscape, rapid change is the norm, and IT organizations must evolve their policies, processes, people and technology accordingly. An agile and flexible IT infrastructure is the order of the day. There are important resource decisions involved with implementing infrastructure changes that need to be assessed more broadly than the IT function (e.g., the in-source, outsource and co-source portions of infrastructure change through the cloud). To illustrate, the cloud provides a dynamic scalable infrastructure that delivers software, platforms and other resources to multiple users (such as employees, customers, suppliers and contractors) without incurring the up-front costs of getting applications up and running. The cloud offers distributed computing over a secure extranet that organizations can deploy without requiring remote access into the corporate firewall. The challenge for IT is to adapt to these changing environments and keep pace with user expectations quickly and efficiently, but not to the point of allowing new systems and architectures to be replaced before realizing the full value expected from the company's investments.
7. **Continuity of critical business processes is the name of the game:** Continuity planning, resiliency and crisis management are vital components of an overall IT risk management program. Directors should inquire of management regarding crisis management and communications, and IT disaster recovery and business process recovery capabilities for the company's critical systems, whether they are owned directly or made available by third parties.
8. **Pay attention to IT security and privacy:** As connectivity of business activity increases, it is critical to view information security and privacy as a business issue because data is an asset that can quickly become a liability if mismanaged either physically or electronically. Security threats, vulnerabilities and privacy exposures challenge every organization, whether they realize it or not, creating risks that must be understood and managed. When organizations do not know the risks

they face, serious threats are left unaddressed that could mushroom into enormous exposures. Boards should ascertain whether management has effective processes in place for identifying and managing security and privacy risks.

9. **Recognize there is a compliance aspect to IT risk:** The organization may have specific compliance requirements affecting IT, and the organization's compliance with many regulatory requirements may require the support of the IT organization. For example, for every legal and regulatory requirement, the organization must ask:
   - What portion of our data does this requirement affect, and are we able to retrieve and maintain this data, as necessary?
   - How do we classify and manage our data in accordance with this requirement?

   The point is that noncompliance with regulatory requirements (including e-discovery requirements) can have severe consequences, and IT plays a role in ensuring compliance.
10. **Deploy leading technology audit methods:** Protiviti's IT Audit Benchmarking Survey, released in November 2013, reported input from more than 460 audit professionals. The study showed that many organizations are perceived as not achieving the IT audit coverage they need, and there remain major shortcomings in IT audit risk assessments.[1]

In summary, lack of IT responsiveness to changing business objectives, a failure to understand the role of IT in the organization, poor alignment of the IT strategy with business goals, an outdated technology infrastructure, and lack of clear information about IT's performance are all factors contributing to an ineffective IT organization. Effective board risk oversight can contribute to strengthening the IT organization so that it maximizes the value IT delivers to the organization.

[1] *From Cybersecurity to IT Governance – Preparing Your 2014 Audit Plan*, Protiviti, November 2013, available at **www.protiviti.com.**

Questions for Boards

Following are some suggested questions that boards of directors may consider, in the context of the nature of the entity's IT risks inherent in its operations:

- Does the board devote sufficient time to IT risks and the organization's capabilities and processes in managing them?
- Does the company monitor technology innovations, including how new technology can be deployed by competitors (or employees) to create disruptive change?
- For significant IT projects, does the board understand the underlying assumptions about how each project produces cost savings, improves business processes or achieves strategic goals, as well as how success will be measured? Is there follow-up to ensure that each significant project delivers on the promises underlying its respective business case?
- Does the board receive adequate information on:
  - The overall costs of IT to the organization?
  - Whether allocations of IT spend across all projects are adequate to ensure optimization of ROI and meet compliance and contractual obligations?
- Does the board understand the data privacy and security risks faced by the company? Are data privacy and security considered an integral part of all new business processes?
- Is the CIO organization effective in supporting the changing needs of the business? For example:
  - Does it review the existing application portfolio periodically to identify opportunities for cost savings and functionality improvements?
  - Are aging legacy systems pre-empting efficiency, agility and innovation?
  - Are cloud solutions being deployed and, if so, does the board understand the risks associated with them?
  - If the company uses outsourced providers, is the board satisfied that such relationships are being managed effectively?
- Does the board take steps to stay current with its knowledge and understanding of IT matters as they relate to the company and the industry?

How Protiviti Can Help

Protiviti works with company executives to maximize return on information systems investments and minimize IT risks. Using strong IT governance and program management practices to ensure alignment with business strategies, Protiviti drives excellence through the IT infrastructure and into supporting applications, data analytics and security. Our comprehensive suite of IT consulting services is focused on: managing the business of IT; managing IT security and privacy; and managing applications and data. Our benchmarking services enable executives to understand IT alignment with business requirements and a cost-effective IT organization.

About Protiviti

Protiviti (**www.protiviti.com**) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 35 percent of FORTUNE 1000® and FORTUNE Global 500® companies. Protiviti and its independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is partnering with the National Association of Corporate Directors (NACD) to publish articles of interest to boardroom executives related to effective or emerging practices on the many aspects of risk oversight. As of January 2013, NACD has been publishing online contributed articles from Protiviti, with the content featured on www.directorship.com/author/jim-deloach/ in the "Blogs & Opinion" section. A compilation of blog posts and articles is maintained and categorized by author's name. Twice per year, the six most recent issues of *Board Perspectives: Risk Oversight* will be consolidated into a printed booklet that will be co-branded with NACD. Protiviti will also post these articles at **Protiviti.com**.

protiviti®
Risk & Business Consulting.
Internal Audit.