Board Perspectives: Risk Oversight

Oversight of Information Technology Risk

Issue 27

Technology continues to evolve at a breathtaking pace, transforming the way people live, interact and work. Companies deploy technology to reduce costs, to improve business processes and, increasingly, to drive revenue expansion. As such, technology is often a key driver of transformational change for companies.

Key Considerations

A recent survey of more than 200 board members determined that 47 percent of directors are dissatisfied with their board's ability to provide IT risk oversight.[1] This statistic is an attention-getter and likely arises from limiting board risk oversight to evaluating individual technology projects as part of approving the capital budget. Consideration of other IT risks has been largely reactive.

Following are suggestions for boards to consider to help them enhance their IT risk oversight:

- **Start with the right questions**: There are three questions boards should ask: What are our risks; how are we managing them; and how do we know? IT risk is both a component of many business risks and an area of specific risk needing evaluation at the enterprise level.
- **Take an integrated, comprehensive view**: Rather than make IT a mere appendage to the board agenda, the board's oversight process should integrate these risks into its 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 cost to IT services, and infrastructure risks. While security and privacy breakdowns and service interruptions get the headlines, IT risk includes other important risks.
- **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 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 strategic planning and execution. Depending on the importance of technology to the sustainability of the strategy, a separate technology committee may be warranted. If there is a separate risk committee, it may also be an option.
- **Understand how technology fits within the business model**: For organizations where technology is a tool for building connections with strategic suppliers, channel partners, customers and outsourcing providers, directors need management to present a picture of IT that is integrated with a view of the business.
- **Remember, there is a compliance aspect to IT risk**: New and expanding regulations continue to

[1] *Taming Information Technology Risk: A New Framework for Boards of Directors*, National Association of Corporate Directors and Oliver Wyman, 2011, page 5, **http://www.nacdonline.org/files/Taming%20Information%20Technology%20Risk%20Final.pdf**.

arise across and within industries. Noncompliance with regulatory requirements can have severe consequences. Therefore, specific compliance requirements necessitate support of the IT organization.

- **Strengthen internal audit**: Protiviti's *2011 IT Audit Benchmarking Survey* (released in October 2011) found that, of almost 500 audit professionals of the companies surveyed, 20 percent lack an IT audit function, 16 percent do not conduct an IT audit risk assessment, and 42 percent lack the resources and skills in audit to evaluate the organization's IT risks.
- **Don't forget board education**: IT risk oversight requires some education for most boards. Directors must look to the CEO, CIO and chief strategy officer for assistance in this regard.

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 processes to manage them?
- Does the company monitor technology innovations, including how new technology can be deployed by competitors (or employees) to create disruptive change? Are aging legacy systems preempting efficiency, agility and innovation?
- For IT projects, does the board understand the underlying assumptions about how each project will produce cost savings, improve business processes or achieve strategic goals, as well as how success will be measured? Is there follow-up to ensure each significant project delivers on promises made?
- Does the board receive adequate information on (a) the organization's overall IT costs and (b) allocations of IT spend across all projects to assess optimization of ROI and ensure compliance and contractual obligations are being met?
- Does the board understand the data privacy and security risks faced by the company? Are data privacy and security considered integral to all new business processes?
- Is the CIO organization effective in supporting the changing needs of the business?
- Are cloud solutions being deployed? If so, does the board understand the risks associated with them?
- If the company uses outsourced providers, is the board satisfied such relationships are being managed effectively?
- Does the board stay current with respect to its knowledge and understanding of IT matters as they relate to the company and industry?

How Protiviti Can Help

Protiviti works with companies to maximize ROI for information systems, minimize IT risks and drive excellence through the IT infrastructure. Our comprehensive suite of IT consulting services is focused on managing the business of IT, IT security and privacy, and 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. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE® 1000 and Global 500 companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half International Inc. (NYSE: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti®
Risk & Business Consulting.
Internal Audit.