If you are a C-suite professional or a board of directors member, you are used to looking at both sides of issues that make their way to your desktop. Likewise, in-depth examination of pros and cons, as well as gaining a full understanding of an issue, is all in a day’s work for internal auditors and is a clear mandate from the audit committee. Seldom will you find more profound benefits or more exorbitant risks in any organization than those accompanying technology. Clearly, technology can support and streamline good processes and operations, but if operations are faulty, or you don’t fully understand their complexity, automating them brings about greater inefficiency and risk. Yet, automating ineffective processes is only the tip of this risk iceberg.

This edition of Tone at the Top looks at technology in the corporate environment and some of the inherent risks that accompany one of the most powerful tools in today’s business world. It also addresses the importance of strict oversight and understanding technology risk in today’s rapidly evolving business culture. What if your lack of understanding of how your organization is leveraging IT is creating risk and under-cutting the opportunities and benefits of its use? Perhaps it’s time to evaluate your approach to IT.

RETHINKING HOW YOU DO BUSINESS

Automating inefficient processes is not the only technology risk that should be on your organization’s radar. What about the risks associated with such 21st century concepts as data security? For example, WikiLeaks made hundreds of thousands of classified government documents available to the general public. How does one calculate the damage of such a breach of information security?

A recent Ponemon Institute study indicates that 90 percent of companies responding to the study suffered data breaches last year. The study results suggest that many organizations are ill-equipped to prevent cyber attacks against their networks and enterprise systems.

RULES OF TECHNOLOGY

“The first rule of any technology used in a business is that automation applied to an efficient operation will magnify the efficiency. The second is that automation applied to an inefficient operation will magnify the inefficiency.”

– Bill Gates, Founder, Microsoft
In an exclusive slideshow on InternalAuditorOnline.org, Steve Mar, director IT Audit for Nordstrom Inc., capsulated the dangers lurking in cyberspace and identified five emerging technology risks:

1. **Social Networking** — Although social networking is growing in use, studies indicate that few organizations have assessed its impact. Companies should develop policies that will adequately address the risks associated with social media such as employee use, breach of confidentiality or theft of intellectual property, and proper brand positioning.

2. **Mobile Computing** — The use of Smartphones, iPads, laptops, personal digital assistants, and other portable devices for work purposes is commonplace. Mobile computing policies should be developed, risks should be assessed, and controls should be implemented and monitored. Common risks to consider are information security, identity theft, and long-term compatibility.

3. **Cloud Computing** — Typically a pay-per-use service, cloud computing is an Internet-provided infrastructure, platform, or software that increases capacity without investment. Risks that should be assessed and monitored include data confidentiality and privacy, data segregation, data integrity, service availability, and regulatory compliance.

4. **Non-alignment of IT and Business Strategy** — If a company’s technological resources do not support the business objectives, those resources are a risk to the company.

5. **IT Infrastructure Attacks by Organized Crime** — Jeopardizing the security of personal information, the stability of business and government infrastructures, and the security and solvency of financial investment markets... These schemes present a real and present danger. After implementing security measures, organizations should test and verify that they are well designed and operating effectively.

Other significant risks are associated with mailing lists, virtual meetings, and bank and credit information. Considering all these technology risks, it’s imperative that organizations simply do not conduct business as they always have. Instead, they must rethink the way they do what they do.

---

**BEING PROACTIVE**

Both the audit committee and internal auditors should have a proactive mindset in regard to technology, as well as all other key risks. This means ensuring that effective controls and security are in place up front. Then, at the point of change, the internal auditors must be there to provide assurance.

Sometimes, after considering the pros and cons of a change initiative, management might move forward in spite of internal auditors’ warnings of increased exposure to risk. In such cases, empowered internal auditors will speak out with their “next best” advice to help limit the organization’s risk exposure. The audit committee should set the tone at the top by encouraging the internal auditors to be proactive.

The internal audit activity should be aware of the situation as soon as the possibility of a change occurs, and the internal auditors should play a part in the process of looking at the feasibility of moving forward. They should be involved in all phases of the process and should assess all key risks.

**INFORMATION SECURITY GOVERNANCE**

Because IT is layered within nearly every aspect of organizations today, only a portion of a company’s technology risks actually occur within the information security (IS) area. However, it is important to include IS governance within this discussion of technology risks.

It is critical that the board of directors and executive management support the governance structure, as effective and efficient IS requires both governance and management actions. Although the board provides overall strategic guidance, management must carry out the board’s directives through day-to-day management and strategic initiative alignment.

As a part of its governance role over the company’s business and organizational risks, the board should ensure IS oversight responsibilities are stated in the charter of the appropriate committee (e.g., the risk committee). The internal auditors should support the designated board committee by providing assurance that relevant policies, procedures, and practices pertaining to IS are in place and operating effectively.

---

**A WORD OF WARNING**

“A fool with a tool is still a fool.”

– Grady Booch, IBM Software Engineer
According to the IIA Global Technology Audit Guide, Information Security Governance, common responsibilities of those involved in governing and overseeing the security of an organization’s information include:

- Promoting good information security practices with clear direction and understanding at all levels.
- Controlling information security risks associated with the business.
- Creating an overall information security activity that reflects the organization’s needs and risk appetite levels.

• How well the chief audit executive (CAE) partners with the chief information officer.
• Whether the CAE is a part of technology feasibility studies and steering groups.
• Whether internal auditing plays a consultative role in regard to projects involving IT systems.
• How the internal auditors keep informed on the changing nature of technology risks and the current level of each risk.
• Whether the internal auditors are proactive in helping the business to manage risk.
• How the internal audit activity goes about assessing risks and controls before issues arise.
• What the internal auditors do in regard to after-the-fact reviews to determine what went wrong.
• Whether the internal audit activity looked at how to make things more efficient.
• What internal auditing does to help ensure the right policies are in place, up-to-date, complied with, and well communicated.

**FOLLOWING BEST PRACTICES**

Clearly, all companies do not have the same tolerance for technology risk. One size does not fit all. For optimal effectiveness, any risk management program should be tailored to meet the risk appetite of the organization. A broad range of risk management and oversight practices have proved effective over time.

Those at the top — executive management, including those overseeing technology, as well as the audit committee of the board of directors — are wise to explore best risk management and technology practices to determine what approaches might be appropriate and applicable to their organization.
The Institute of Internal Auditors (www.theiia.org) is dedicated to the global promotion and development of internal auditing.

Established in 1941, The IIA is an international professional association with global headquarters in Altamonte Springs, Fla. The IIA has more than 170,000 members in internal auditing, risk management, governance, internal control, IT auditing, education, and security.

The IIA is the global voice, recognized authority, chief advocate, principal educator, and acknowledged leader in certification, research, and technological guidance for the internal audit profession worldwide. The IIA enhances the professionalism of internal auditors and is internationally recognized as a trustworthy guidance-setting body. It fosters professional development, certifies qualified audit professionals, provides benchmarking, and through The IIA Research Foundation, conducts research projects and produces educational products.