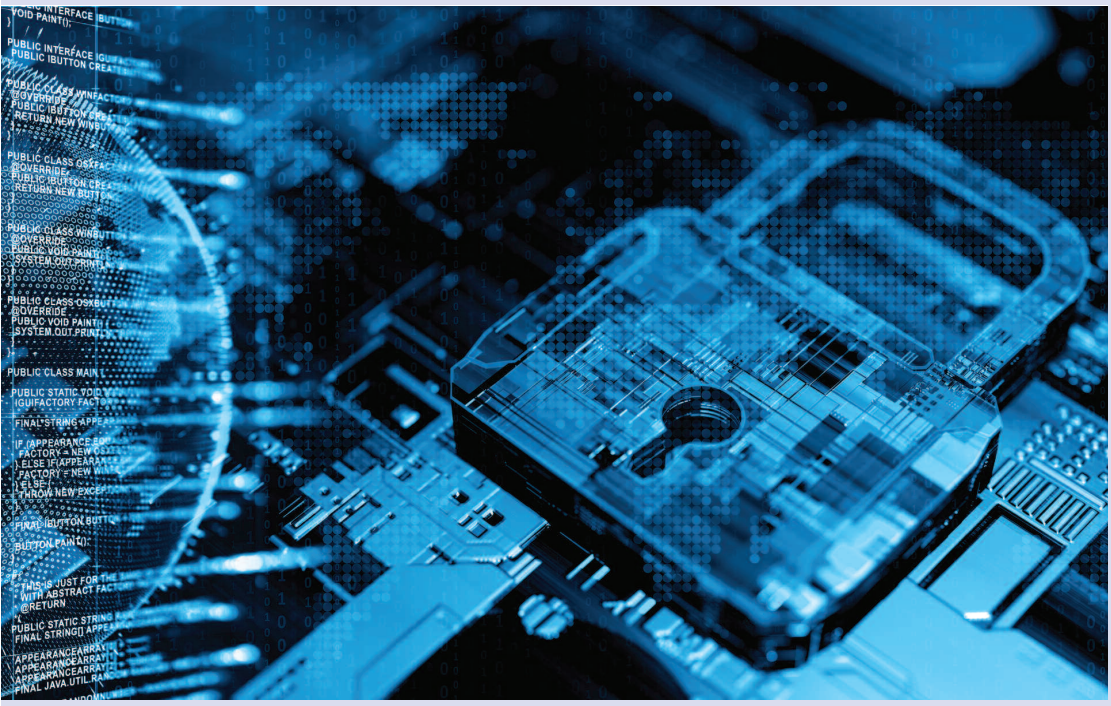
Enterprise Technology Risk in a New COSO ERM World

Eight Challenges Facing Management

By Joel Lanz

The release of the revised Committee of Sponsoring Organizations (COSO) *Enterprise Risk Management—Integrated Framework* (https://www.coso.org/Pages/erm-integratedframework.aspx) could not have come at a better time for technology risk professionals and those concerned with effectively and efficiently managing that risk. Executives can no longer manage technology risks from an IT department silo; rather, they require an integrated enterprise risk management (ERM) approach—as suggested by the framework—that considers the impact of technology risk in the strategy-setting process, as well as in driving performance. This article discusses some of the more challenging technology risks facing managers due to their enterprise-wide impact or consideration.



Defining Risk Appetite

Perhaps one of the greatest challenges facing technology risk managers is the concept of risk appetite. The COSO ERM framework's glossary defines "risk" as "the possibility that events will occur and affect the achievement of strategy and business objectives" and "risk appetite" as "the types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value." Companies accept that to achieve business objectives and strategies, they must have an online presence and leverage technology to drive efficient and competitive service delivery strategies. These same technologies, however, can also cause significant damage to an entity's reputation and lead to lawsuits. Quantifying technology risk appetite presents greater challenges to risk managers, who consider technology risk as "all or nothing"—that is, either a breach occurs or not—as opposed to financial risk, which focuses on risk-adjusted returns. For example, many companies have zero tolerance for being breached, although preventing all breaches may require an unreasonable investment or substantial expense.

Companies benchmark and

quantify their practices against industry standards or guidance (e.g., PCI Security Standards, Center for Internet Security Controls, ISO, CoBIT) to manage risk in a prudent business fashion. Although not always quantifiable, these standards provide a baseline against which organizations can define their risk appetite or target. Alternatively, some companies use a maturity model (e.g., based on Gartner or CMMI guidance) to benchmark or step-level targets; risk appetite is then defined by how well the company is managing its technology risk as compared to others.

When considering the risks discussed in this article and applying the guidance to specific situations, it is important to remember this challenge as well as the general practices used in one's specific industry, as a company's risk appetite is directly related to these factors. The COSO ERM framework's authors realized and appreciated the impact of technology on enterprise risk; in the "Looking into the Future" section of the executive summary, they identified that organizations would continue "to face a future full of volatility, complexity, and ambiguity." They also identified four illustrative trends influencing enterprise risk management, each having significant technology implications: dealing with the proliferation of data; leveraging artificial intelligence and automation; managing the cost of risk management; and building stronger organizations. The following sections describe how these relate to technology risks and affect the enterprise's overall risk profile.

Cybersecurity

For many organizations, cybersecurity threats and oversight continue to demand attention from senior executives and boards of directors. Reputable researchers, as well as industry and professional organizations, continue to release surveys identifying cybersecurity as a top enterprise risk concern. These same groups provide training for board members to help them satisfy their governance obligations. Expected losses that could result from data breaches, theft of intellectual property, reduced sales, regulatory sanctions, and, most importantly, potential damage to market reputation have fueled investment in risk reduction strategies.

Despite these investments, challenges remain. Cybersecurity has made technology a consistent topic of discussion during board and audit committee meetings, providing IT risk professionals, including information security officers and chief information officers, with the opportunity to gain exposure at the board level and to seek board support for investments in necessary efforts to mitigate cyber threats. Even with this support, the risk remains; moreover, for many at the board level, it is a frustrating risk. Unlike other business risks, where management makes investments to remediate the problem and then resolve it, cybersecurity risks tend to remain and, in some cases, increase due to the evolutionary nature of cyber threats. Recent incidents that suggest the involvement of governmental entities and targeted attacks by hacktivists have only increased both the challenge and frustration. The cycle continues as, despite the increasing threats, businesses have limited resources to deploy and must continue to invest in protection in a prudent, business-focused manner. An indirect concern is the diversion of board focus and resources to cybersecurity while ignoring other technologies or business risks requiring their attention.

Unlike other business risks, where management makes investments to remediate the problem and then resolve it, cybersecurity risks tend to remain and, in some cases, increase due to the evolutionary nature of cyber threats.

Perhaps this area best benefits from the guidance provided in the new COSO ERM framework. Realistically, 100% cybersecurity protection cannot be achieved; however, understanding the organization's risk appetite and aligning investments with strategic goals can increase managerial effectiveness. One example is exiting or not providing certain services whose risk/reward exceeds established risk tolerances. Other enterprise risk mitigation strategies include aligning operations with a minimum baseline security standard, periodic reporting on vulnerabilities and patch management activities, and implementing an appropriate testing strategy to help ensure that a company's actual cybersecurity profile reflects business objectives and expectations. Moreover, appropriate enterprise-wide measurement, testing, and oversight increase the effectiveness of the training received by company personnel (e.g., to prevent clicking on malware or responding to phishing scams).

Data Governance

Outside of cybersecurity, perhaps no other enterprise-related IT risk management topic has captured executive management and board attention like data governance. From an enterprise perspective, which users or departments own the company's data, what they can do with it, and how they should protect it have always been topics of discussion and, in some cases, sources of conflicts. The recent scandal at Facebook involving data acquired by the company and sold to third parties has increased attention paid to this concern. Although definitions of data governance vary, the definition provided by the

National Institute of Standards and Technology (NIST) is generally used to initiate discussions at various levels of a company. According to the NIST definition, data governance is "a set of processes that ensures that data assets are formally managed throughout the enterprise. A data governance model establishes authority and management and decision-making parameters related to the data produced or managed by the enterprise" (http://bit.ly/2J0XM1R).

The data governance challenge begins with a historical perspective that did not view data by itself as something that required board oversight and enhanced controls. Concern always existed on using data to process financial transactions or to support financial statement presentation. Data like a customer list was usually considered proprietary or confidential, and the greatest risk envisioned was that a sales executive would take that information to a competitor. The accumulation of customer data, however, whether through the maturing capabilities of customer relationship management (CRM) or other databases and big data analysis tools, enabled companies to accumulate much more information about their customers. For some companies, the sale of this information became a new revenue stream with no royalty and, in some cases, no notification to the customer. In some industries, services or information were provided to customers in exchange for tracking their data and eventually selling it to advertisers (e.g., social media and search engines). In addition, regulatory expectations [e.g., the EU's General Data Protection Regulation (GDPR)] and other privacy expectations continue to rise.

The problem facing most companies is that while data is an asset, most of them do not treat it as such. Until recently, most companies did not inventory the data they maintained, its source, or to whom they were giving or selling the information. Within the company, ownership of the data and the responsibility for its use was subject to the company's internal political environment. Complicating the issue is the use of spreadsheets and users' ability to contract with cloud service providers, further bypassing organizational controls. The tide does seem to be turning: companies have started to inventory and prioritize the protection of the data they have, and managers continue to develop new policies communicating enterprise expectations and monitoring adherence to policies. Other efforts include software to monitor the transmission of sensitive information, enhanced data analysis tools to identify unusual data movement and activity, and risk management consideration of vendor and other third-party contracts that involve sensitive information.

The problem facing most companies is that while data is an asset, most of them do not treat it as such.

Vendor Management & Cloud Computing

For many organizations, cloud computing has been a game-changing development, especially for small- to mid-size businesses (SMB). Companies appreciate the ability to purchase services as needed, to use software that larger competitors use, not to be limited by infrastructure or investment cycles, and to take advantage of continuously upgraded software without having to make significant investments. These benefits enable companies to respond to market opportunities and meet increasing customer demands. Financial executives also appreciate the ability to better match expenses with income and not to have to own and amortize computer hardware and software services.

Cloud computing has grown so popular and useful that technology companies to whom SMBs outsource their systems (i.e., cloud service providers) now use cloud providers such as Amazon Web Services (AWS) and Microsoft Azure themselves to deliver services cost effectively and minimize the potential of loss from the most pervasive threats. Such vendors will often advertise and promote the reputation of AWS and Azure in selling their services; often, if the SMB does due diligence or vendor management over its vendor, it relies on the vendor's representation that using AWS and Azure provides "best-in-class" security to the customer.

Both AWS and Azure communicate that security is a joint responsibility between the organizations and the technology service provider, and that, as part of its vendor management oversight, the endpoint customer should determine and confirm that its technology service provider is addressing those responsibilities. For example, AWS distinguishes between its responsibilities and those of providers. As described on its website:

> AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services ('Security of the Cloud'). Customer responsibility will be determined by the AWS Cloud services that a customer selects. The document helps define the amount of configuration work the customer must perform as part of their security responsibilities ('Security in the Cloud'). (https://amzn.to/2LpUYK4)

To assist customers in understanding and testing their responsibilities, AWS provides extensive tools and guidelines, including a "Risk and Compliance Whitepaper" and an "Introduction to Auditing the Use of AWS" (https://amzn.to/2kkpxo2). From an enterprise risk perspective, companies should ensure that their third-party service providers are complying with and managing the requirements specified by AWS in these documents. Azure provides similar documentation and customer support, which its users should also follow.

End User Responsibilities

Many organizations continue to delegate technology responsibilities to their business units; as these business units are closer to the customer, their ability to influence technology decisions and effectively use technology resources to provide customer service and hopefully generate new sales opportunities makes sense. In some respects, organizations have traditionally held users accountable for their use of technology, although frequently this was in name only. In many organizations, management expects the central IT department to provide significant support and, in many cases, "hand-hold" business owners to meet their needs and mitigate any circumvention of controls not compensated for by pervasive IT department practices and expertise.

Technology developments such as cloud computing, mobile technology, and data analytics have pushed technology decisions and responsibilities further into the user community. In many cases, outside of providing general technology-related expertise and guidance, the central IT function can no longer control what the user does or what type of information is maintained and used. The ability to extract data from centrally protected core systems significantly increases the technology risk profile related to the integrity of the information. This spike in risk is no longer limited to traditional uses of information, such as financial statement reporting; the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), GDPR, and other privacy-related laws and regulations that impose strict expectations and significant penalties on companies to protect data entrusted to them by consumers. Moreover, business expectations increasingly demand that end users take charge and make risk management happen in order to achieve strategic business objectives.

As with most business demands, these expectations, opportunities, and compensation come with responsibilities. End-user risks include challenges that businesses have been trying to resolve since the advent of the computer era. As they take on responsibilities for computing within their departments, users must still effectively mitigate many of the threats and risks that reside within their departments. These include traditional general controls such as segregation of duties, application acquisition and implementation, operational resiliency, and logical security. End users must also ensure that software includes appropriate application controls, whether as part of a cloud computing solution or a desktop spreadsheet or database tool. Determining the completeness and accuracy of input, correctly calculating and processing formulas and algorithms, and securing the resultant output can significantly affect the reliability of information used for managing the enterprise and protecting its reputation. Other enterprise risks include ensuring that users are aware of their responsibilities and periodically reporting relevant metrics and information to those charged with governance to help ensure that they provide the appropriate oversight.

Artificial Intelligence and Automation

The evolution of data analytics and its acceptance by senior executives and boards have paved the way for the use of artificial intelligence and related automation to enhance technology's ability to solve and better address business objectives and challenges. As organizations continue to adapt and rely on these tools, however—especially for critical decision support—technology risk managers need to identify and manage their risks as well. Realization of these results could result in decisions that damage the long-term viability of the company.

Critical risk considerations for these tools center around traditional development and application controls. Can the company rely on the controls used in the tool's development process, and is the analysis and resultant calculation reliable? Are the data sources used for the analysis accurate and timely? Do processing and analysis consider all the data processed and exclusions?

From an ERM perspective, a consistent strategy needs to be adopted. As with end-user computing, educating and communicating common expectations are critical for areas that involve the accuracy and reliability of results, such as user acceptance and stress testing.

As organizations continue to adapt and rely on these tools, technology risk managers need to identify and manage their risk as well.

The Cost of Risk Management

The cost of seizing new business opportunities and entering new markets is an increase in a company's risk profile. While

most agree on the necessity of managing this increased risk, there is general disagreement on the quantity of risk management needed and which risk mitigation activities provide minimal value to the enterprise, including those procedures that are duplicative. Most business executives, however, understand the need for these controls. The recent focus on extensive documentation requirements also raises significant concerns related to the cost and added value of risk management provided.

Frameworks provide companies with consensus practices and guidance on how best to manage risk. When using a single framework, the cost of documenting compliance with that framework can sometimes be justified (although still controversial), as it demonstrates the organization's due diligence when exercising its fiduciary responsibility to protect shareholder assets. Unlike financial reporting, where there is a consensus around one framework (e.g., COSO), many different frameworks address technology risk and cybersecurity. As a result, the effort involved in juggling multiple frameworks increases the total cost of managing risk. Recognizing this challenge, many of the frameworks include cross-references that facilitate the use of multiple frameworks when needed.

Another concern relates to "checking the box." In this risk mitigation approach, management implements multiple controls based on the items in a checklist. The results often include the excessive management of threats or the implementation of controls that do not adequately manage the risk in question. Risk professionals generally agree that fewer controls that target specific risks are preferable and more cost beneficial than implementing large catalogs of controls.

The technology risk management profession continues to try to introduce and adopt risk metrics to better manage investments and related costs. In some cases, traditional financial metrics such as return on investment and security spend per employee have been used with some success. Other attempts at metrics include those focused on achievements, including attacks prevented and percentage of users trained. The challenge remains, however, to define generally recognized and accepted tools to justify the investments made by corporate management and the board.

Risk professionals generally agree that fewer controls that target specific risks are preferable and more cost beneficial than implementing large catalogs of controls.

Building Stronger Organizations

People drive organizations, and the same is true when it comes to effective and efficient technology risk management. Organizations of all sizes continue to invest in technology risk management in general and in cybersecurity capabilities in particular; examples include recruiting appropriately trained professionals with a combination of risk management and technical skills. The lack of qualified staff and the increased demand for these skills have generally raised salaries and bonuses paid to these professionals when hired. In addition, given their importance to the enterprise, these professionals are no longer limited to reporting within the IT function, but rather are viewed as a second line of defense, with a typical reporting to a chief risk officer.

Because of staffing challenges, organizations continue to partner with specialist advisors who can enhance a company's risk management posture. Contracted services can range from outsourcing the entire security operations to contracting for a chief information security officer (CISO) on an as-needed basis, also known as a virtual CISO (vCISO). Efforts to strengthen risk management practices throughout the enterprise also include enhanced awareness and technical training for employees. Of note is a renewed appreciation for making sure that employees are trained and qualified in the technology that they use to help ensure that they perform their tasks securely, efficiently, and effectively.

Eliminating all human risk is not possible, but disciplined risk approaches can result in loss reductions. Consistently applying the disciplined approach promulgated by the COSO ERM framework throughout an organization will enable it to better prepare employees to manage evolving threats and risks and become a stronger organization.

Meeting the Challenge

The ability to manage technology risk is a critical component of any organization's ERM effort. COSO's new *Enterprise Risk Management–Integrated Framework* provides companies with the flexibility and tools needed to align technology risk with strategic goals and business objectives. Cybersecurity threats and computer errors will always be factors that hinder an organization's success, reputation, and value. The new ERM framework provides a process for companies to make appropriate investments for the given risk appetite and tolerances, helping to ensure that risk-adjusted returns provide necessary funding for the long-term well-being of the enterprise. ❑

Joel Lanz, CPA/CGMA/CITP/CFF, CISA, CISM, CISSP, CFE, *is the founder and principal of Joel Lanz, CPA, P.C., Jericho, N.Y. He is a member of* The CPA Journal *Editorial Advisory Board.*