4-1-2006

Is IT Next for ERM? Information Technology Provides the Vital Infrastructure for Building a Modern Enterprise

Sridhar Ramamoorti
University of Dayton, sramamoorti1@udayton.edu

Marcia L. Weidenmier

Sridhar Ramamoorti, PHD, CIA, ACA, CPA, CFE, CFSA, CRP, CGAP, CGFM
Marcia L. Weidenmier, PHD, CPA

As the waves of change caused by the U.S. Sarbanes-Oxley Act of 2002 subside, the next force likely to sweep over organizations is the need to implement enterprise risk management (ERM). ERM has sparked a paradigm shift by encouraging organizations to build a comprehensive risk strategy into their business operations and spurring internal auditors to move from a primarily control-based approach to a predominantly risk-based approach.

One major area of enterprise risk that internal auditors must understand is how information technology (IT) affects their organization within the context of The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) Enterprise Risk Management—Integrated Framework. IT is intertwined with all eight components of COSO's ERM framework—as both a source of risk and a risk management tool (see "ERM Automation" on page 47). Internal auditors also can add substantial value to the organization by providing advice on using IT to develop a sound ERM program. Auditors must first understand how technology impacts each component of the ERM framework.

Internal Environment

The internal environment sets the overall tone of the organization's response to risk and provides an actionable basis for all other components of COSO's ERM framework. It includes the organization's ethical values, risk appetite, ERM philosophy, and the competence and development of its employees, as well as how the organization views risk and implements controls. Risk appetite is the level of risk that an organization is willing to accept, which affects its choice of IT, e-commerce strategy, and use of emerging technologies. Such technology decisions not only change the organization's risks, but also make them more complex. For example, the moment an organization engages in e-commerce, it becomes "global," even if its operations are geographically confined to one country. As a result, organizations that sell products and services online must address a host of security, confidentiality, and privacy risks and technology compatibility issues that they might not face if they only did business through traditional retail channels.

Objective Setting

According to COSO ERM, the organization's mission and risk appetite drive its objective-setting process, which defines high-level strategic objectives and the corresponding operating, financial reporting, and compliance objectives needed to accomplish them. Strategic objectives affect the organization's selected IT infrastructure and risk level. IT, however, influences organizational objectives in a sort of "chicken and egg" way: It can drive as well as enable organizational strategy. But IT also generates new risks that may require technology solutions. For example, organizations that use e-mail to communicate and manage knowledge must establish appropriate IT protocols, passwords, and authentication procedures to keep messages secure.

Moreover, IT is critical to using operational assets effectively and ensuring the integrity and reliability of the organization's financial reporting system. IT can help organizations comply with

applicable laws and regulations, especially the Sarbanes-Oxley Act's sweeping requirements. Indeed, many publicly listed companies rely on IT-based controls and real-time data collection and analysis to facilitate compliance with Sarbanes-Oxley sections 302 (attesting to the integrity of financials), 404 (internal control over financial reporting), and 409 (near-real-time reporting of material changes). The extensive organizational information-gathering effort requires enterprisewide systems, such as enterprise resource planning (ERP) applications and data warehouses, to extract and analyze data for trends and relationships among the data.

Internal auditors can also use technology to collect and analyze performance measures to ensure that the organization is operating within its acceptable risk-tolerance level. Embedded audit modules that perform exception reporting, for example, can call attention to processing of transactions of more than US $1 million for all business units or listing transactions that are duplicative, represent sales returns, or exceed a certain established number or value of vendor/customer transactions per month. Auditors can easily specify such exception-reporting criteria as part of their financial reviews and use automated tools to scrutinize nonroutine, and flagged, journal entries.

Event Identification

COSO ERM highlights the unique role that IT plays in identifying events or incidents that may affect the organization's ability to achieve its objectives. Events maybe characterized as negative risks or positive opportunities. COSO contends that IT is the only factor that can be viewed as an external or internal event, while functioning as an "environmental scanner" to identify other events.

When viewing IT as an external event, an organization must consider the positive and negative effects that its e-commerce environment and new technology can have on the business. Although new technologies and services can enhance the availability of data and lower infrastructure costs, they also can increase demand for technology-based services and cause service interruptions. Moreover, these advances can disrupt the organization's business model and relationships with suppliers, customers, and other business partners. For example, American Airlines' SABRE system revolutionized the airline industry's ticketing process — enabling consumers to book their own flight reservations and issuing electronic tickets — but adversely impacting travel agents. Similarly, the viability of publishing companies like Encyclopaedia Britannica has been threatened by free and low-cost Internet-based information sources.

When viewing IT as an internal event, an organization must determine how volume volatility; data integrity; data and system availability; and system selection, development, deployment, and maintenance may affect its operations. Consider the impact that an internal event, the introduction of a "self-service" employee application system called Green Tree, has had at Edward Hospital & Health Services in Naperville, Ill. Green Tree has transformed the hospital's employee recruiting and selection process by giving hospital recruiters the ability to handle large numbers of potential employment candidates. However, the hospital's process of software selection, development, deployment, and maintenance, as well as training human resources employees, has proven time-consuming and costly.

Technologies such as data warehouses, event inventories, workshop facilitation software, process flow software, and exception reporting can help internal auditors recognize internal and external events. Data warehousing and data mining can facilitate customer relationship management (CRM) and supply chain management (SCM) — two of the most critical types of business interactions involving supply and demand — allowing organizations to identify top customers and suppliers and analyze the natutre and length of those relationships. Such information enables organizations to assess customer and supplier satisfacition, evaluate the benefits and potential risks of the relationship, and better understand key issues for negotiation. Many organizations have made large investments in CRM and SCM systems and have hired outside consultants to implement them. Auditors, in turn, can review their organization's return on investment from these technology streamlining endeavors.

Risk Assessment

COSO ERM characterizes risk assessment as a continuous process of estimating the likelihood of potential events and their impact on the organization. Likelihood is the possibility or probability that an event will occur, while impact is the financial outcome of the event. New technologies and e-commerce have made IT a significant and evolving source of business risk that must be assessed. Estimates of the likelihood and impact associated with IT risk may change frequently as technology changes and systems become increasingly integrated across organizations and their business partners. For example, new viruses emerge each day with the potential to interrupt or shut down an organization's operations and any integrated system. Newly discovered operating system flaws create potential security holes that put organizational data and reputation at risk. Constant advances in IT also can make new systems obsolete before they go live.

However, IT also can be a valuable risk-assessment tool. For example, internal auditors can mine internal, external, and industry benchmarking data to estimate the likelihood and impact of an event. Tools such as simulation, modeling, stress testing, scenario analysis, and optimization can estimate the various financial impacts of different time horizons and probability models. To comply with operational risk measures required by the revised Basel Capital Accord, beginning in 2007, many financial services organizations will rely on complex technology applications, such as integrated databases and rules-based risk management engines, to monitor enterprise credit, market, and operational risk. Meanwhile, sophisticated technology platforms and associated software applications will facilitate financial modeling of discounted cash flows, as well as derivatives, swaps, and options strategies.

To direct attention to high-risk audit areas, auditors may use artificial intelligence (AI) or neural networks, which make scenario-specific predictions by recognizing patterns in data through a "learning" process similar to that of the human brain. Recent advances in technology have produced powerful Al applications, although these products require a fair amount of customization to meet the specific needs of auditors in a particular industry.

Risk Response

Following the risk assessment phase, COSO ERM discusses the need for an appropriate organizational risk response to ensure that the residual risk is within the acceptable risk-tolerance level. Residual risk is the risk that remains after considering the organization's risk response.

Organizations may select one of several responses to IT risk — avoidance, sharing, reduction, or acceptance. To avoid IT risks, an organization may minimize IT usage, steer clear of e-commerce and emerging technologies, and reduce the number of IT contact points with the outside world. The organization may opt to share the risks by augmenting its standard insurance with supplemental insurance that covers network-related incidents and other IT risks that are not part of their policy's property, commercial general liability, and crime coverage. If the organization decides to reduce IT risks, internal auditors need to make sure strong IT controls that can alter the organization's risk profile are established. For example, sound software patch management procedures that ensure the latest features and security updates are incorporated can reduce the risk that systems may be compromised internally or externally or operate inefficiently. Finally, if an organization determines that the inherent IT risks are within its risk-tolerance level, no action is required. Instead, the organization would simply factor those risks into the level of "self-insured risk" it is willing to assume.

When selecting a risk response, the organization must analyze the costs and benefits of reducing the likelihood and impact of the risk. This cost-benefit analysis should be conducted from a portfolio viewpoint that examines all interrelated risks, because risks across the organization may counterbalance or exacerbate each other. By definition, ERM calls for viewing risks at a "macro level." Organizations can calculate financial risks and rewards globally and by strategic business unit, taking into account short- and long-term cash flow positions as well as foreign exchange translation and conversion issues. This analysis also can help manage treasury risk by forecasting cash flow needs over a defined period based on projections, assumptions, and estimates. Technology tools can assist in this analysis and the organization's risk management decision-making process.

Control Activities

COSO ERM describes control activities as the policies, procedures, processes, and monitoring mechanisms that ensure the selected risk responses are in place and determined appropriately. The internal audit function can play a pivotal role by helping the organization define manual and IT controls to prevent, detect, and correct potential problems. Built-in preventive IT controls in the form of input edit checks can automatically ensure that transactions are complete, accurate, authorized, and valid. Similarly, organizations must confirm and validate the existence and operating effectiveness of general and application controls. This is especially true after a new system is implemented, because built-in access controls often are turned off or are not fully deployed to get the system up and running as fast as possible.

Streamlined ERP processes may alter and weaken established segregation of duties, traditionally a primary preventive control. Unlike a manual system that physically separates tasks, an ERP system automatically integrates organizational tasks. If the system does not define user authorizations appropriately, the same employee maybe able to make unauthorized purchases because there is no control that prevents that person from initiating a purchase, receiving the

goods, and matching the goods to the vendor's invoice. Similarly, if a user maintains master files, such as vendor records, and initiates transactions, the organization is also vulnerable to purchases from unauthorized and fictitious vendors.

Internal auditors can use audit software as a detective control to identify incomplete, inaccurate, or potentially fraudulent data. Corrective controls, such as IT control mapping and alarms or alerts, can enable auditors to monitor control effectiveness and changes within ERP systems continuously. Where key controls are weak or missing, auditors should ensure that compensating controls are in place.

Controls should be designed to support each of the organization's strategic, operational, reporting, and compliance objectives. When assessing the effectiveness of existing internal controls, auditors need to understand the link between objectives, potential risks, and control activities that should be in place to mitigate those risks. An organization's control environment is effective only if all links are clearly understood and functioning.

Information and Communication

IT is the basis of the COSO ERM information and communication component. Reliable, timely information is needed to identify, analyze, and respond to risks. ERP systems, in conjunction with integrated data warehouses, can collect, process, and seamlessly distribute vast amounts of internal and external data for ERM in a short time. IT also can be used to communicate needed information across all levels of the organization. Auditors can help ensure that ERP and other systems are filly integrated so that information flows quickly — vertically, horizontally, upstream, and downstream — throughout the organization. This integration can prevent organizations from being bogged down by information fragmentation and bottlenecks and allow decision-makers to keep up with the rate of change in the organization's internal and external environments.

Depending on the organization's risk-tolerance level, internal auditors may need to monitor the integration of data systems across the supply chain. To reduce costs, organizations may choose to send data and funds electronically, as well as give business partners access to their systems to share inventory, production, and other needed data. Although information sharing can increase the efficiency and effectiveness of operations, internal auditors must be cognizant of the additional risk exposure the organization could face if sensitive and confidential information is released to third parties without authorization. In recent years, several well-known financial services and retail companies have acknowledged that confidential customer data stored electronically has been stolen or otherwise compromised; the U.S. Federal Trade Commission fined data broker Choice-Point US $15 million in January for failing to protect customer data.

Monitoring

COSO's ERM framework considers the monitoring function to be critical for any effective ERM implementation. In today's rapidly changing business environment, the organization's ERM plan must change constantly to ensure that the organization is always controlling risk effectively. This requires ongoing monitoring that is real-time, dynamic, and embedded in the organization. For

example, to maintain segregation of duties, any changes to user access privileges should be logged automatically for further review. Although large organizations may have the personnel and other resources needed to meet this need, technology tools give organizations of all sizes a greater ability to monitor enterprise risks. Digital agents and software modules can identify exceptions and extract data automatically for data mining and analysis, automated variance analysis, reconciliations, and comparisons.

The rapid pace of IT and organizational change places greater pressure on internal auditors to pay close attention to how IT impacts their organization's ERM process. Auditors must understand the organization's systems, infrastructure, programs, processes, and constituents; record and evaluate controls over critical and sensitive information; assess monitoring procedures; and obtain external assurances. Internal audit participation throughout the systems development life cycle may also reduce IT risk, as long as auditors do not jeopardize their independence and objectivity.

Finally, internal auditors can help develop information systems to provide the board of directors with mandated financial information, industry insights, and risk and controls analysis. By understanding the organization's current and future uses of IT, internal auditors can help implement and assure the most effective ERM process possible for their organization.

ERM Automation

Although it increases enterprise risk, it can also help organizations manage and mitigate risks. One method is to develop an automated reporting system with built-in IT controls that identifies security breaches, attempts to misstate business performance, and changes in the financial, operational, and compliance reporting environment. This could be accomplished by embedding audit modules that facilitate continuous monitoring and exception reporting. For example, software tools can retrieve real-time financial information from online sources that conforms with the eXtensible Business Reporting Language (XBRL), which uses standardized Web-based tags for reporting financial and business information. The U.S. Securities and Exchange Commission is currently experimenting with allowing companies to submit 10-K filings in XBRL.

Knowledge management systems (KMS) can also enhance risk management by capturing, developing, and distributing knowledge that helps organizations solve problems and make decisions. KMS integrate technologies such as data warehouses, data mining, online analytical processing, intelligent agents, group-ware, and neural networks. Many organizations use these systems to collect customer feedback and other information to assess the "intangibles-driven value" of service efforts and accomplishments that cannot be quantified easily. As a risk management tool, KMS can capture organizational knowledge including best practices, external contacts, lessons learned, and frequently asked questions. An effective KMS should include knowledge mapping features that visually display captured information and the relationships between the information components. Internal auditors must ensure that knowledge is constantly produced, captured at the source, analyzed within a data warehouse, and transmitted immediately to the appropriate users.

Technology-savvy internal auditors can play a significant role in the design and implementation of technologies such as KMS and XBRL, but the same auditors should not provide assurance on such systems after they are launched. Instead, a different group of auditors must review and evaluate the success of the systems.