Internal Controls and Managing Enterprise-Wide Risks

By John Farrell

In addition to complying with the sweeping reforms in corporate governance and financial reporting following the Sarbanes-Oxley Act, companies can benefit further by adopting a broader view that encompasses an enterprise-wide risk-management outlook. This approach is especially applicable to section 404 of the Sarbanes-Oxley Act, which deals with management's assertion regarding the effectiveness of its internal controls over financial reporting. As companies work to comply with these new rules, they can build their section 404 work into an opportunity to address other aspects of risk throughout the organization, including financial, legal, and operational.

The emerging trend of evaluating and monitoring the range of business risks—including those assessed in an internal control review—may help companies simultaneously meet strategic goals, boost shareholder and stakeholder value, and focus on good governance.

Self-Assessment

Fulfilling the mandates of section 404 need not be an obstacle to implementing an enterprise risk-management effort. Instead, the compliance process can enable companies to focus on enterprise-wide risks through a distributed evaluation—that is, a self-assessment of risk and control. This evaluation assigns responsibility for the assessment to those who are "closest to the action"—in other words, those most directly involved in the control over each process. Such an approach can help companies achieve a better-balanced risk and control status.

Conventional wisdom formerly held that responsibility for internal controls was delegated to an organization's financial group. According to current thinking, however, internal controls are owned by those within the business who manage daily operations and who depend on the controls for achieving their goals. These control process owners are well prepared to perform the distributed evaluation of identifying, evaluating, and managing pertinent risks to assist the business in achieving its financial goals. The Sarbanes-Oxley rules reinforce the value of such risk-based evaluations.

If a company looks ahead one year, how can it measure success beyond mere compliance with regulatory requirements? For multinational companies, one sign of success would be a worldwide standardization of internal controls that allows the organization to orient itself toward a widely accepted set of control criteria, such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO) internal control framework or the COSO enterprise risk-management (ERM) framework issued in 2003. Coining a "controls language" shared throughout the organization can help a company take greatest advantage of its set of controls—deciding which key controls to keep and which it can discard because they do not add value or are otherwise unnecessary.

Process Improvement

In addition, companies may use the section 404 assertion rules to help them achieve a company-wide transformation of business processes. The internal-control assessment may produce several improvements:

- Greater use of automated, or system-based, controls;
- Better evaluation of process risks and mitigation of risk;
- More uniform controls throughout the organization; and
- Greater responsibility for controls assessment for the process owners.

The compliance procedures can also be used to weed out nonessential tasks and determine good practices within each business process:

- Comparing controls between different business units, or within a company's operations in different countries;
- Cutting the risk of error by using a more technology-based method of control rather than manual processes;
- Using key performance indicators to gauge the effectiveness of a process across a span of risks and time periods; and
- Getting feedback from control procedures on a worldwide basis, which can lead to better reporting capabilities.

In examining their sets of controls, companies may find it valuable and cost-effective to consider an automated system rather than a manual review. The internal control assessment, performed through an automated self-assessment, is more than a simple questionnaire. It can gather information from control owners about the status of key controls. The assessment is based not on the frequency of the assertion but on the type of control—automated or manual—and how vulnerable to risk the controls may be.

Using an automated system for internal control assessment offers several other advantages. It consolidates internal control information and status, as well as being a repository of all organizational risks and controls. The repository is useful not only for section 404 reporting responsibilities but also for any ERM initiatives.

Role of the Internal Auditor

The internal auditor can play a vital role in linking internal control reporting with ERM. The internal auditor can foster an environment that allows the company to link the efficiencies of an ERM approach to the overall business aims of the organization.

In addition to articulating the linkage of internal control reporting with ERM to senior management, the internal auditor can perform a number of other important functions:

- Helping control process owners gain a better understanding of internal control assessment and testing.
- Becoming a purveyor of best practices within the organization. For example, if the internal auditor discovers that a particular business segment has adopted a more efficient approach to internal control reporting, she can share that knowledge with other business segments.

■ Generally enhancing the organization's understanding of internal controls by imparting subject-matter knowledge in this area.
■ Monitoring the organization's internal controls through testing and feedback on its control status.

Focus on Governance

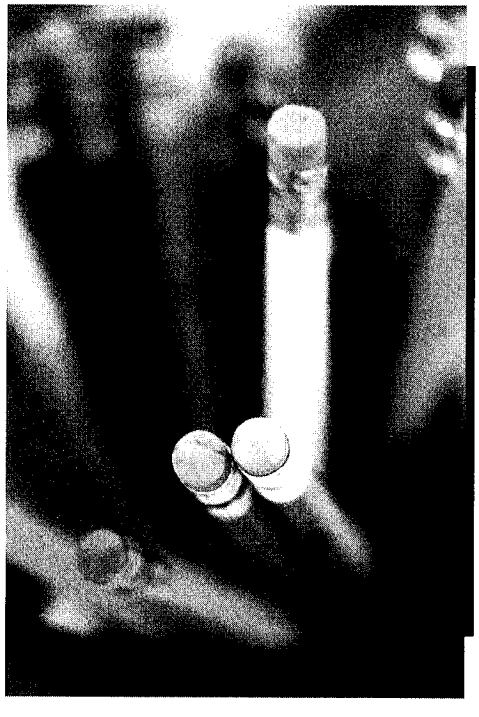
While the distributed evaluation, or risk assessment, is properly assigned to the operations people with direct experience in their respective areas, the overall risks that an organization faces continue to be a corporate-governance priority for the board of directors and management. To help them better understand those risks, corporate leaders should consider the following questions:
■ What types of analyses is the organization doing to identify risks?
■ What is the organization doing to assess those risks and find the best way to take advantage of or mitigate them?

In response to the mandates and recommendations of Sarbanes-Oxley, senior management may consider several other measures to enhance corporate accountability:
■ Assessing self-knowledge and knowledge of others in the organization.
■ Ensuring that a uniform process exists and is followed by other members of the organization that provides internal certification.
■ Assessing the impact of changes in the business that may have an effect on internal controls; for example, acquisitions or divestitures, and new accounting or SEC rules.
■ Obtaining formal internal management representation letters, on a quarterly basis, from internal accounting personnel for domestic and foreign subsidiaries.
■ Holding monthly or quarterly conference calls with accounting staff (including worldwide operations) to review new accounting pronouncements and other items that facilitate the closing process.
■ Initiating a formal regular meeting with key process owners or segment leaders (including sales, purchasing, human resources, and legal) to discuss activities that may influence accounting and disclosure.
■ Harmonizing these measures with any ERM initiatives.

Applying an ERM approach to the internal-control assessment process has costs. It may be more costly, however, not to seize the opportunity to implement this approach. The investment would include:
■ Establishing a risk framework and common risk vocabulary;
■ Establishing and maintaining a chief risk officer or risk committee;
■ Continued measuring and monitoring; and
■ Periodic updating of the risk assessment framework.

For many companies, a phased-in approach is the most practical way to deal with the cost issue. Initially, a company evaluates only the risks and controls over financial reporting, but it designs the evaluation tools and techniques so they can support ERM. Once the evaluations required by Sarbanes-Oxley are complete, the company can expand the assessment into the operational and strategic realms, until a complete ERM system is in place. ❑

John Farrell, CPA, *is a partner in the internal audit services practice of KPMG LLP, and is based in New York City. He can be reached at 212-872-3047 or at johnmichaelfarrell@kpmg.com.*



Let Us Hear From You

The CPA Journal welcomes letters from readers in response to articles published in the magazine as well as those concerning issues of general interest to the accounting profession. Although we receive more letters than we are able to publish, all letters receive consideration.

The editors reserve the right to edit letters for clarity and length. Writers should include their contact information, including a daytime telephone number and an e-mail address, if possible.

Letters may be addressed to Letters to the Editor, The CPA Journal, 530 Fifth Avenue, 5th Floor, New York, N.Y., 10036, or to cpaj-editors@nysscpa.org.