7-2003

COSO: More Relevant Now than Ever

Heather M. Hermanson
Kennesaw State University, hhermans@kennesaw.edu

Recommended Citation
Hermanson, Heather M. "COSO: More Relevant Now than Ever." Internal Auditing 18.4 (2003): 3-6.

COSO: More relevant now than ever
Hermanson, Heather M
Internal Auditing; Jul/Aug 2003; 18, 4; ProQuest Central
pg. 3

COSO: MORE RELEVANT NOW THAN EVER

As the details of the Sarbanes-Oxley Act's requirements for reporting on internal control are hammered out at U.S. public companies, many are turning to the COSO internal control framework for answers.

HEATHER M. HERMANSON

In 1992 when the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued its internal control framework, few would have guessed that the framework would become an integral part of corporate accountability a decade later, but things are moving in that direction. COSO's framework may become an important tool for implementing the directives set forth in the Sarbanes-Oxley Act of 2002. While the framework has been lauded for its comprehensive model of internal control, most executives have failed to embrace the Treadway Commission's recommendation of reporting on internal control effectiveness. Without monitoring and accountability for control effectiveness, the framework is tantamount to a diet without weigh-ins.

With the newly mandated reporting on controls and other directives set forth in the Sarbanes-Oxley Act, the full effect of COSO's internal control vision may finally be realized. COSO's framework may help to address compliance with the new internal control reporting requirements. Although the primary focus of the COSO report is internal control, the framework has implications for other areas of the Sarbanes-Oxley Act as well.

The SEC's implementation of the Sarbanes-Oxley Act

Section 404 of the Sarbanes-Oxley Act mandates annual reporting by management on the effectiveness of internal controls. The external auditors must attest to these annual internal control reports. On May 27, 2003, the SEC adopted rules to implement the requirements of Section 404. Most filers must comply with the new internal control reporting requirements beginning with fiscal years ending on or after June 15, 2004. The SEC rules require management to issue an annual internal control report that includes:

- a statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company;
- management's assessment of the effectiveness of the company's internal control over financial reporting as of the end of the company's most recent fiscal year;
- a statement identifying the framework used by management to evaluate the effectiveness of the company's internal control over financial reporting; and
- a statement that the registered public accounting firm that audited the company's financial statements included in the annual report has issued an attestation report on management's assessment of the company's internal control over financial reporting.[1]

As indicated above, the rules require management to identify the framework used for evaluating the effectiveness of the organization's internal control. The rules allow for any "suitable, recognized control framework that is established by a body or group that has followed due-process procedures, including the broad distribution of the framework for public comment."[2] The SEC recognized the COSO framework as satisfying its requirements. However, the SEC did not mandate a particular framework,

---

HEATHER M. HERMANSON, Ph.D., CPA, is a professor of accounting at Kennesaw State University in Georgia, where she teaches courses in financial accounting and auditing. Her previous research on internal control reports has been published in Accounting Horizons *and* Internal Auditing.

COSO INTERNAL CONTROL FRAMEWORK

Information about the COSO internal control framework is available online at www.coso.org. The excerpts below are from this site.

"Internal control is broadly defined as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- **Effectiveness and efficiency of operations.**
- **Reliability of financial reporting.**
- **Compliance with applicable laws and regulations."**

Control Environment: "The control environment sets the tone of an organization, influencing the control consciousness of its people. . . . Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people; and the attention and direction provided by the board of directors."

Risk Assessment: "Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed . . . ."

Control Activities: "Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties."

Information and Communication: "Pertinent information must be identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. . . . All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. . . ."

Monitoring: "Internal control systems need to be monitored—a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. . . . Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board."

primarily because other evaluation frameworks exist outside the United States.

Unfortunately, without a common framework, financial statement users will incur a greater burden in comparing and interpreting reports using different frameworks. However, U.S. companies should find the COSO framework to be a good fit for Section 404 compliance, and the SEC appears to have adopted its rules with COSO in mind.

Concerns about the SEC's proposal on Section 404

According to comment letters received by the SEC, two major concerns emerged from the SEC's original proposal for internal control reports: the lack of an internal control framework and the minimal time estimates for implementation.

Commentators were concerned that the lack of a particular control framework would result in parties not agreeing on a common definition of internal control. Though the SEC did not adopt the COSO framework in the final rules, it did adopt a definition of internal control over financial reporting consistent with a subset of the COSO definition of internal controls. Thus, use of the COSO framework for reporting on internal controls seems to be a natural interpretation.

Commentators also were concerned about the SEC's estimated time burden for reporting on internal controls. In the original proposal, the SEC estimated the burden for quarterly and annual internal control reports at approximately ten hours per quarterly and annual report (five hours for disclosure controls and five hours for remaining financial reporting controls). Given the low time estimates and the lack of a proposed framework, some companies may have perceived that the internal control reporting requirements were purely superficial.

The final rule recognizes a far greater average annual burden for reporting on internal controls: 383 hours per company (even this is low for larger companies). The SEC virtually eliminated the proposed quarterly evaluation requirement (unless a company has a material change to controls). This reassessment of the burden appears to recognize the magnitude of an evaluation under an accepted framework such as COSO.

COSO's internal control framework: a great solution

The SEC's final rule acknowledges but does not mandate the COSO framework as a suitable evaluation tool for internal control reporting. In addition, the COSO framework may help with some of the Sarbanes-Oxley Act's other directives as well. This is because COSO offers a comprehensive view of internal control that involves everyone from directors to employees. The framework:

- defines internal control;
- describes its components;
- provides criteria against which an assessment of internal control can take place;
- gives guidance on external reporting; and
- supplies materials useful in conducting an evaluation of the control structure.

The COSO framework project was supervised by a group comprised of executives (Financial Executives International), managerial accountants (Institute of Management Accountants), internal auditors (The Institute of Internal Auditors), external auditors (American Institute of Certified Public Accountants), and academics (American Accounting Association). Four key features make the COSO internal control framework a useful tool for implementing Sarbanes-Oxley Act directives: the framework is established, evaluative, simple, and dynamic.

Established. The COSO framework developed a common definition for internal control. COSO defines internal control in terms of three broad categories of objectives: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with laws and regulations. This definition of internal control was adopted by the AICPA for evaluation of control risk in financial statement audits in Statement on Auditing Standards (SAS) No. 78 and by large banks in their implementation of the FDIC Improvement Act (FDICIA) of 1991. Thus, its use is already widespread. Companies adopting the COSO framework may reduce costs to financial statement users who do not need to familiarize themselves with a new framework. Also, by focusing on this well-established definition of internal control over financial reporting in its final rule, the SEC likely minimized confusion about internal control terminology.

Evaluative. COSO acknowledges that determining whether a control system is effective is a subjective judgment. However, the framework provides a means of making that judgment through the evaluation of five interrelated components:

1. control environment;
2. risk assessment;
3. control activities;
4. information and communication; and
5. monitoring.

Each of these components must be present and functioning effectively in order for the system to be judged effective. Thus, the components also serve as the criteria for effective internal control.

The framework not only describes the criteria, but offers a complete volume of evaluation tools. These tools include worksheets for each of the five components. Each worksheet provides the key "points of focus" for the particular component. The worksheets are designed to help management evaluate the specifics of each component and develop an assessment of the control structure as a whole.

Having a benchmark for effective controls promotes consistency in evaluation and reporting across companies. Companies adopting the COSO framework will mitigate concerns raised in comment letters to the SEC about consistent application of the term "effective controls." These companies will have defined criteria for concluding their controls are effective, and they will have the tools necessary for making the evaluation.

Simple. COSO's longevity may be due in large part to its simplicity. The core model of five interrelated components is easy to recall and understand. Its pyramid structure, where control environment is the foundation and monitoring is the pinnacle, is intuitive. The simplicity of the model affords non-accountant users an opportunity to grasp the basic concept of control effectiveness. Thus, reporting on internal controls under this

FOUR KEY FEATURES MAKE THE COSO INTERNAL CONTROL FRAMEWORK A USEFUL TOOL FOR IMPLEMENTING SARBANES-OXLEY ACT DIRECTIVES: THE FRAMEWORK IS ESTABLISHED, EVALUATIVE, SIMPLE, AND DYNAMIC.

framework should result in users' enhanced understanding of the report.

Dynamic. The COSO framework continues to be updated for a changing business environment. After the initial framework was issued, COSO developed new guidance for internal controls in derivative usage. Currently, COSO is focusing on managing enterprise risk. That project is developing improved risk identification and risk analysis procedures that may be incorporated into the framework. COSO hopes to have an exposure draft of the project available on its website (www.coso.org) by July 15, 2003. With a focus on the future, the COSO framework is a dynamic tool.

COSO's application beyond Section 404

Though the COSO framework was designed to help management evaluate internal control effectiveness, it may help with other Sarbanes-Oxley Act directives as well. Given the comprehensive nature of the model, an effective control structure under COSO should increase the chances of a reliable information system for management and the board of directors to use (particularly if the complete definition of control is adopted). Thus, the system should provide audit committees with useful information for carrying out their duties per Section 301 of the Act. In particular, an effective control structure would help to ensure that the audit committee receives pertinent information about accounting and auditing problems or complaints. Also, an effective system under COSO would help to ensure that officers receive reliable financial information such that they would feel more confident certifying the financial statements under Section 302 of the Act. Finally, the continued monitoring of the control system required under the COSO framework should minimize companies' exposure to criminal penalties under Titles VIII, IX, and XI of the Act. If companies monitor their controls and adjust them for changes in the environment, they should have a stronger defense against Sarbanes-Oxley Act violations.

The directives of the Sarbanes-Oxley Act present many challenges to companies and their management teams. The COSO framework can help them to meet these challenges. ■

NOTES

1 SEC Final Rule No. 33-8238 (June 5, 2003).

2 *Ibid.*