Board Perspectives: Risk Oversight

COSO 2013: What Have We Learned?

Issue 76

The updated COSO Internal Control – Integrated Framework was issued in May 2013. Since its release, several important lessons have been learned, a few of which we consider in this article.

Key Considerations

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued its updated Internal Control – Integrated Framework (Framework) almost three years ago. Since then, its implementation has been an important endeavor for many companies listed on exchanges in the United States in their efforts to comply with Section 404 of the Sarbanes-Oxley Act of 2002 (SOX). As background, the U.S. Securities and Exchange Commission (SEC) requires companies to use a "suitable framework" as a basis for evaluating the effectiveness of internal control over financial reporting (ICFR), as required by Section 404. The COSO Framework meets the SEC's criteria for suitability. Accordingly, many companies have transitioned from the previous framework to the updated version.

No doubt Section 404 compliance is important, as it relates to maintaining effective ICFR. However, as important as the lessons learned in this critical area are, there are other important lessons that should be of interest to boards as directors consider the relevance of internal control to their risk oversight endeavors. Below, we undertake a high-level look at some of these lessons.

The control environment is vital to preserving an organization's reputation and brand image – Since the release of the COSO Framework, there have been a number of corporate scandals related to operational, compliance and reporting issues. While we're not in the business of calling out the companies involved (some of them well-known), we are confident that every director has his or her own list of companies that have been besieged by persistent negative headlines that define an unfortunate chapter of their legacy. These companies likely lacked a strong control environment in the areas that contributed to the crisis.

A critical component of internal control, the control environment lays the foundation for a strong culture around the organization's internal control system. The control environment consists of the policies, standards, processes and structures that provide the basis for carrying out effective internal control across the organization. Through their actions, decisions and communications, the board of directors and senior management establish the "tone at the top" regarding the importance of internal control. Management reinforces expectations at the various levels of the organization in an effort to ensure alignment of the tone in the middle with the tone at the top.

According to the COSO Framework, the control environment comprises the:

- Organization's commitment to integrity and ethical values;
- Oversight provided by the board of directors in carrying out its governance responsibilities;
- Organizational structure and assignment of authority and responsibility;
- Process for attracting, developing and retaining competent people; and
- Rigor around performance measures, incentives and rewards to drive accountability for performance.

Without a supportive culture and effective management support at all levels for internal control, the organization is susceptible to embarrassing control breakdowns that could tarnish its reputation and brand image. This issue is likely a contributing factor at the companies that have been hit recently with headline-grabbing scandals.

The control environment applies to outsourced processes – Organizations typically extend their activities beyond their four walls through strategic partnerships and relationships. The blurred lines of responsibility between the entity's internal control system and those of outsourced service providers create a need for more rigorous controls over communication between the parties. For example, information obtained from outsourced service providers that manage business processes on behalf of the entity, and other external parties on which the entity depends for processing its information, should be subject to the same internal control expectations as information processed internally.

The point is clear: Management retains responsibility for controls over outsourced activities. Therefore, these processes should be included in the scope of any evaluation of internal control over operations, compliance and reporting, to the extent a top-down, risk-based approach determines they are relevant. Controls supporting the organization's ability to rely on information processed by external parties include:

- Vendor due diligence;
- Inclusion of right-to-audit clauses in service agreements;
- Exercise of right-to-audit clauses;
- Obtaining an independent assessment over the service provider's controls that is sufficiently focused on relevant control objectives (e.g., a Service Organization Controls Report, typically referred to as a SOC 1 Report); and
- Effective input and output controls over information submitted to and received from the service provider.

The potential for fraud should be considered explicitly when conducting periodic risk assessments – Ongoing risk assessments are an integral part of a top-down, risk-based approach to ensuring effective internal control. In these assessments, directors should ensure that management evaluates the potential for fraudulent financial and nonfinancial reporting (e.g., internal control reports, sustainability reports and reports to regulators), misappropriation of assets, and illegal acts. In addition, the potential for third-party fraud is a relevant issue for many organizations. As the COSO Framework points out, fraud risk factors include the possibility of management bias in applying accounting principles; the extent of estimates and judgments in reporting; fraud schemes common to the industry; geographical areas where the organization operates; performance incentives that potentially motivate fraudulent behavior; potential for manipulation of information in sensitive financial and nonfinancial areas; entering into unusual or complex transactions; existence or creation of complex organizational structures that potentially obscure the underlying economics of transactions; and vulnerability to management override of established controls relating to operations, compliance and reporting.

There are important lessons learned in Section 404 compliance – Quality public reporting is like the sleeves of a shirt. If the shirt is well-laundered and looks nice, no one notices. Smear some dirt and grime on one of the sleeves, and everyone sees it. The analogy is relevant to financial reporting because investors take reporting fairness for granted; however, when public companies restate previously issued financial statements for errors in the application

of accounting principles or oversight or misuse of important facts, investors notice. The bottom line is that the markets take quality public reporting at face value. Once a company loses the investing public's confidence in its reporting, it's tough to earn it back.

Section 404 compliance is important in the United States because material weaknesses in ICFR provide investors early warning signs of financial reporting issues. We have gleaned many lessons in our work successfully transitioning numerous companies to the 2013 COSO Framework from the 1992 version. The most important of these lessons is that a top-down, risk-based approach is vital to Section 404 compliance. Some companies forgot to apply this approach when setting the scope and objectives for using the updated Framework; as a result, they went overboard with their controls testing and documentation. We can't stress strongly enough that the 2013 COSO Framework did not change the essence of and need for a top-down, risk-based approach to comply with Section 404.

Other lessons include:

- Meet with your external auditor early and often to ensure that the company is fully aligned with the auditor on the appropriate process for transitioning to the updated Framework.
- Establish an effective and relevant mapping approach to link established key controls to the principles outlined in the COSO Framework by leveraging the points of focus provided by the Framework; start with existing controls documentation, and consider the nature of the Framework's components.
- Manage the level of depth when testing indirect controls (often referred to as entity-level controls) by focusing on the specific objectives germane to ICFR; for example, for the indirect control emphasizing background checks, management should scope the application of this activity to the appropriate people designated with financial reporting responsibilities rather than all employees throughout the organization (unless management wishes to expand scope beyond financial reporting).
- Focus on understanding and documenting control precision by understanding the control's track record in detecting and correcting errors and omissions to support an assertion that the control effectively meets the prescribed level of precision.
- Evaluate the completeness and accuracy of information produced by the entity to support the execution of key controls; the Public Company Accounting Oversight Board (PCAOB) inspection reports are driving auditors to place more audit emphasis on validating system reports, queries and spreadsheets.

Application of the 2013 COSO Framework to operational, compliance and other reporting objectives is virgin territory – In applying the updated COSO Framework, most organizations have limited their focus to ICFR. Some organizations even believe that the Framework was designed exclusively for Section 404 compliance. Such is not the case. There are benefits to using the Framework for other objectives relating to operations, compliance and other reporting. However, these efforts should be segregated from Section 404 compliance. Progressive organizations are applying the COSO Framework to other areas, such as sustainability reporting, regulatory compliance and controls over federal grants, to name a few.

Questions for Boards

Following are some suggested questions that boards of directors may consider, based on the risks inherent in the entity's operations:

- Have directors paid close attention to whether the organization's control environment is functioning effectively?
- Does the organization periodically consider fraud risk in its risk assessments? Is the board satisfied that the risk of third-party fraud is reduced to an acceptable level?
- Does the company's process for complying with Section 404 apply a top-down, risk-based approach, and is the process cost-effective?
- Has management considered applying the COSO Framework to improve internal control in areas other than financial reporting?

How Protiviti Can Help

Protiviti assists boards and executive management with assessing the risks inherent in the enterprise's strategy and business plans, both across the entity and at various operating units, and the internal controls and other capabilities for managing those risks. We help organizations identify and prioritize the risks that can impair their reputation and brand image and lead to failure to execute the corporate strategy successfully. We assist organizations in applying the COSO Internal Control – Integrated Framework to operations, compliance and reporting.

About Protiviti

Protiviti (**www.protiviti.com**) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. Protiviti and our independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Named one of the 2015 *Fortune* 100 Best Companies to Work For®, Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Protiviti is partnering with the National Association of Corporate Directors (NACD) to publish articles of interest to boardroom executives related to effective or emerging practices on the many aspects of risk oversight. As of January 2013, NACD has been publishing online contributed articles from Protiviti, with the content featured on www.nacdonline.org/Magazine/author.cfm?ItemNumber=9721. Twice per year, the six most recent issues of *Board Perspectives: Risk Oversight* will be consolidated into a printed booklet that will be co-branded with NACD. Protiviti will also post these articles at **Protiviti.com.**

protiviti®
Risk & Business Consulting.
Internal Audit.