

Board Perspectives: Risk Oversight

COSO 2013: Why Should You Care?

Issue 58

The updated COSO *Internal Control – Integrated Framework* has been out for more than a year. This year, many companies are beginning to use it to evaluate their internal control over financial reporting (ICFR) to comply with Section 404 of the Sarbanes-Oxley Act of 2002.¹ Two questions arise with respect to the board:

- Why should directors care about this framework?
- What do they need to know about it?

Key Considerations

Much has been written about the 2013 updated COSO framework by large accounting firms, major business publications and various newsletters. Like its original 1992 counterpart, the updated framework depicts five components of internal control: control environment, risk assessment, control activities, information and communication, and monitoring. Seventeen principles drawn directly from these components add rigor to the framework with fundamental concepts. According to COSO, an organization achieves effective internal control by determining that each of the five components and all relevant principles are in fact present and functioning in providing reasonable assurance that objectives

Six Reasons Why Directors Should Care

Boards influence the “tone at the top.”

Boards are responsible for oversight of the control environment.

Boards are responsible for oversight of the other four internal control components.

Internal control weaknesses matter.

Boards need to pay attention to the risks of management override, fraud and illegal acts.

Your company may be transitioning to the updated framework soon.

are achieved, regardless of whether the objectives apply to operations, reporting or compliance.

There are six reasons why the board (or one or more of its committees) should care about the updated framework. **First, boards influence the “tone at the top” in any organization.** The COSO framework emphasizes the importance of the tone at the top and the board’s responsibility for overseeing the development and performance of internal control. While there is no doubt that the tone at the top is shaped primarily by the CEO’s operating style and his or her team’s personal conduct, it is also true that directors exercise significant

¹ Our *Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements – Frequently Asked Questions Regarding Section 404* (Fourth Edition) is available at www.protiviti.com/en-US/Pages/SOX-404-FAQs.aspx.

BOARD PERSPECTIVES: RISK OVERSIGHT

influence over the organization's attitude toward risk, the aggressiveness of its policy choices and its commitment to responsible business behavior. These considerations send a message to the organization.

Second, the board is responsible for oversight of the control environment. The significance of the framework is that it defines the control environment over which directors have substantial influence. The control environment ensures the organization acts with integrity; the board demonstrates independence from management and exercises appropriate oversight; management establishes (with board oversight) structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives; the organization attracts, develops and retains competent people; and the organization holds people accountable for results.

To illustrate the board's oversight of the control environment, the framework provides that directors:

- Oversee the definition and standards of the organization's conduct, establish expectations and evaluate CEO performance and integrity;
- Ensure that, as a governing body, they have the requisite skills and are sufficiently independent to provide effective oversight;
- Provide effective challenge to executive management, as necessary, by asking the tough questions regarding proposed plans, deals, and significant and unusual transactions; and
- Seek input and support from independent risk management and compliance functions, internal auditors, external auditors, and others.

A strong control environment should be a priority of the board because it lays the foundation for the organization to position itself to be more resilient in the face of internal and external pressures.

Third, the board is also responsible for oversight of the other four internal control components. For example, according to the COSO framework, the board:

- Considers internal and external factors that pose significant risk to the achievement of objectives, and evaluates and challenges management's assessment

of risks inherent in new strategic initiatives, such as pursuing new markets or proposed acquisitions or innovating facilities and processes;

- Inquires as to the effectiveness of the design and operation of control activities in reducing risk to an acceptable level in critical areas;
- Communicates direction and tone at the top to executive management; obtains information relating to the company's achievement of objectives from both internal and external sources; reviews disclosures to external stakeholders for completeness, relevancy and accuracy; and encourages upward communication of significant matters; and
- Assesses the nature and scope of monitoring activities, any management overrides of established controls, and management's evaluations and remediation of control deficiencies.

Fourth, internal control weaknesses matter. Directors instinctively know this. There is empirical evidence as well:

- **Strong controls reduce financial restatement risk:** A 2013 Audit Analytics® research report, *2012 Financial Restatements: A Twelve Year Comparison*, shows that the number of restatement and non-reliance disclosures in the United States peaked in 2006, steadily declined through 2009, and has been "relatively stable" since. The required reporting on the effectiveness of ICFR was a significant contributor to this trend, as it added discipline to the control structure.
- **Effective controls improve stock price:** A study released in May 2006 by Lord & Benoit reported that shareholders benefit when companies have effective ICFR. To illustrate, for the period from March 31, 2004 to March 31, 2006, the Russell 3000 share index increased by 17.7 percent. The Lord & Benoit study found that companies reporting no material weaknesses in ICFR for either 2004 or 2005, and companies reporting material weaknesses in 2004 but no material weaknesses in 2005, enjoyed a 27.7 and 25.7 percent increase in share price, respectively. However, companies reporting material weaknesses in *both* 2004 and 2005 suffered a 5.7 percent *decline* in share price.

BOARD PERSPECTIVES: RISK OVERSIGHT

The above examples apply to financial reporting controls. When effectively designed, controls over operations and compliance also add value in terms of ensuring strong quality, time, cost and innovation performance, as well as avoiding unwanted incidents that result in a reputation hit.

Fifth, the board needs to pay attention to the risks of management override, fraud and illegal acts.

The board is the last line of defense on matters involving management overriding established controls for an illegitimate purpose, including personal gain or “cooking the books.” The updated framework makes it clear that “management override” should not be confused with “management intervention,” which represents overt actions management undertakes because existing controls fail to address unanticipated circumstances. Such actions are typically disclosed to appropriate personnel, whereas management override is not. The framework recommends that the board (or a board committee) oversees management’s assessment of the risk of override and challenges management as circumstances dictate. In addition, the framework states that management should assess risk in areas susceptible to fraud and illegal acts and improve controls in those areas, and the board should provide input on such assessments.

Sixth, if your company accesses the capital markets in the United States, it will be transitioning to the updated framework soon. The only question is when. COSO recommends transitioning to the 2013 updated framework by fiscal years beginning after December 15, 2014, at which time COSO will consider the 1992 version superseded. Thus, for calendar-year companies, this would mean completing the transition in 2014. The U.S. Securities and Exchange Commission (SEC) hasn’t issued an official position on the transition question insofar as compliance with Sarbanes-Oxley Section 404

is concerned. However, the SEC staff has indicated that it intends to monitor the transition for issuers using the 1992 framework to evaluate whether any further action is appropriate at some point in the future.

We encourage companies to complete the transition in accordance with COSO’s guidance. Those companies choosing to defer the transition run the risk of receiving a comment letter from the SEC staff. If the company receives advice from its external auditor indicating that it can delay the transition until the following year, management should ask the auditor whether the audit staff will use the principles and points of focus provided by the 2013 updated framework in auditing the effectiveness of ICFR of audit clients electing to continue using the 1992 framework. Management should also obtain input from legal counsel on any decision to delay the transition.

Questions for Boards

The board of directors, or the appropriate board committee, may want to consider the following questions in the context of the nature of the entity’s risks inherent in its operations:

- What are the major changes COSO has made to the *Internal Control – Integrated Framework*, and how will those changes affect the company in using the framework?
- How does the 2013 updated framework impact management’s approach to complying with Sarbanes-Oxley Section 404? Are there any potential deficiencies or matters for the board to consider in terms of its oversight of internal control?
- What is management’s plan and supporting rationale for transitioning to the 2013 updated framework? What are the disclosure ramifications if management intends to use the superseded 1992 framework this year?

BOARD PERSPECTIVES: RISK OVERSIGHT

How Protiviti Can Help

Protiviti assists organizations with applying the COSO *Internal Control – Integrated Framework* in conjunction with their financial reporting, other reporting, operations and compliance objectives. We advise companies and their boards on strengthening the control environment, enhancing risk assessment processes, and improving the control structure and monitoring activities.

For additional guidance on the 2013 updated framework, we invite you to go to www.protiviti.com/en-US/Pages/The-Updated-COSO-Internal-Control-Framework-FAQ.aspx and download a complimentary copy of our resource guide, *The Updated COSO Internal Control Framework: Frequently Asked Questions (Third Edition)*. This guide addresses various questions regarding the updated framework, including the reasons why it was refreshed; what has changed; the process for transitioning to its use; and steps companies should take now.

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 40 percent of FORTUNE 1000® and FORTUNE Global 500® companies. Protiviti and its independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies.

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.directorship.com/author/jim-deloch/ in the “Blogs & Opinion” section. A compilation of blog posts and articles is maintained and categorized by author’s name. 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.