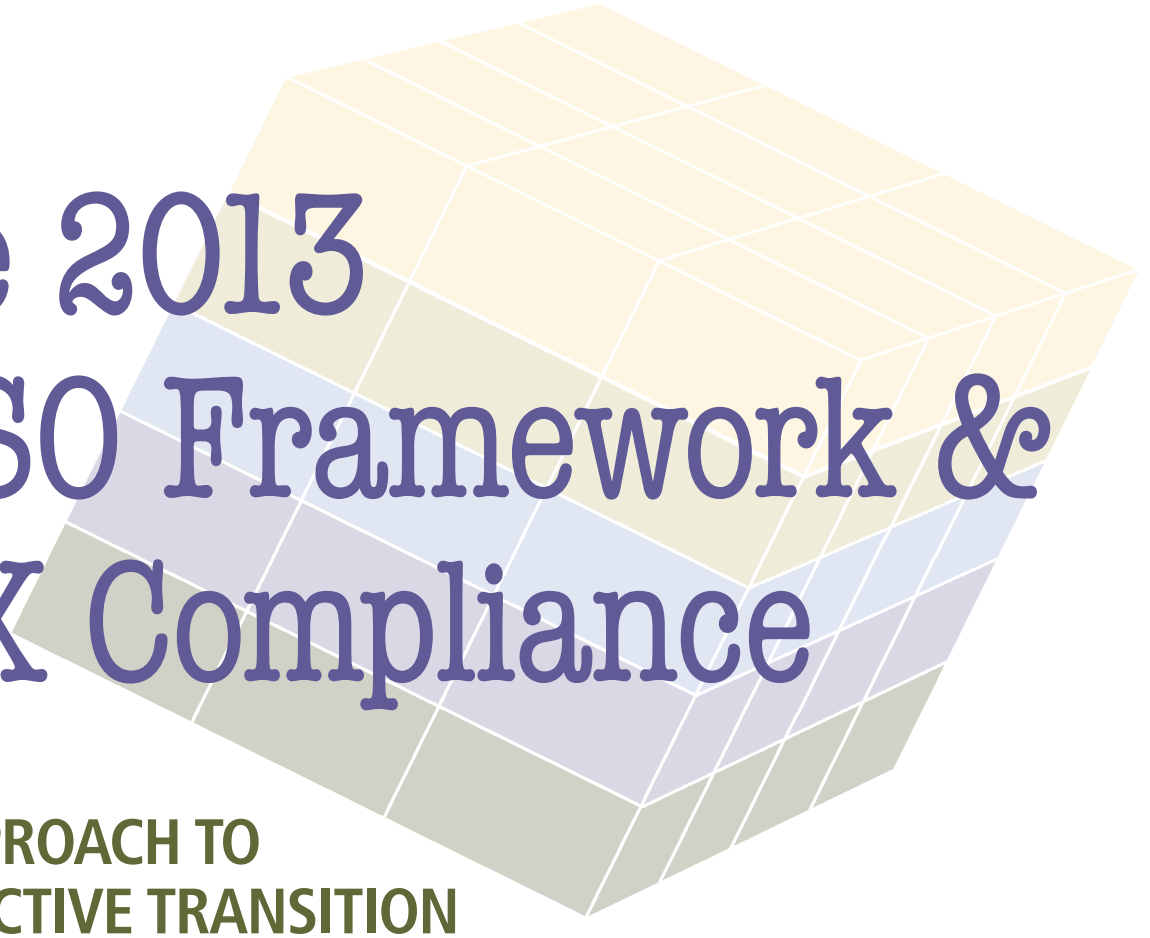
COSO
COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

ima®
The Association of Accountants and Financial Professionals in Business

The 2013 COSO Framework & SOX Compliance

ONE APPROACH TO AN EFFECTIVE TRANSITION

By J. Stephen McNally, CPA



The 2013 COSO Framework & SOX Compliance

ONE APPROACH TO AN EFFECTIVE TRANSITION

By J. Stephen McNally, CPA

Do you work for a publicly traded company that's subject to Sarbanes-Oxley Act (SOX) Section 404 compliance requirements? If so, odds are high that you're familiar with the *Internal Control—Integrated Framework* that was published in 1992 by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). As you know, SOX 404 requires management at public companies like Campbell Soup to select an internal control framework and then assess and report on the design and operating effectiveness of their internal controls annually. The majority of U.S. publicly traded companies have adopted COSO's 1992 Framework to do this.

As a quick reminder, COSO is a voluntary private-sector initiative dedicated to improving organizational performance and governance through effective internal control, enterprise risk management, and fraud deterrence. Five nonprofits are its sponsoring organizations: AAA (American Accounting Association), AICPA (American Institute of Certified Public Accountants), FEI (Financial Executives International), IIA (Institute of Internal Auditors), and IMA® (Institute of Management Accountants).

On May 14, 2013, COSO released an updated version of its *Internal Control—Integrated Framework*. Why was the Framework updated and to what end? Is adoption of the 2013 Framework required for SOX 404 compliance? How can you make an efficient and effective transition from the original 1992 Framework? How soon do you need to complete your transition? This article provides answers to these questions; an overview of COSO's 2013 Framework, authored by PwC; and one approach, including specific steps, on how to transition an entity's SOX compliance program to the updated Framework.

Overview

COSO's new Framework is the result of a significant multiyear project—including two rounds of public exposure—to review, refresh, and modernize the original Framework, ensuring it remains relevant. As we all know, the world has undergone a seismic shift since 1992 that has led to dramatic business and operating environment changes. Markets continue to globalize. Business models have changed significantly, including greater use of shared services and outsourced service providers. The complexity and pace of change in rules, regulations, and standards have intensified demands on companies. Reliance on evolving technology—increasingly important in improving business performance, business processes, and decision making—continues to grow. Finally, regulators and other stakeholders have higher expectations regarding governance oversight, risk management, and the detection and prevention of fraud. While advances have been made in better connecting risk management and internal control practices in pursuit of organizational strategic goals, the many changes since 1992 have significantly increased business risk, resulting in a much greater need for competence and accountability than ever before.

In addition, collectively we have learned lessons in applying the 1992 Framework. First, the original Framework included lengthy discussions of internal control concepts that are now institutional knowledge. Second, although the concept of internal control principles may have been embedded in the original Framework, the principles themselves were "hidden" within the details. Third, practitioners have used the Framework primarily for internal control over external financial reporting, yet the Framework encompasses three major categories of objectives, including operations, overall reporting, and compliance objectives. Thus, streamlining the original Framework; codifying the underlying principles; increasing focus on operations, nonexternal financial reporting and compliance objectives; and enhancing usability were additional drivers behind COSO's *Internal Control—Integrated Framework* (ICIF) Refresh Project.

The Case for Transition

Throughout this multiyear project, the COSO Board has emphasized that the key concepts and principles embedded in the original Framework remain fundamentally sound for designing, implementing, and maintaining systems of internal control and assessing their effectiveness. Therefore, COSO will continue to make the original Framework available through December 15, 2014, at which time the 1992 Framework will be considered superseded. During this transition period—today through December 15, 2014—COSO believes continued use of the 1992 Framework is acceptable. Entities leveraging COSO's *Internal Control—Integrated Framework* for external reporting purposes during the transition period, however, should clearly disclose whether they used the 1992 or 2013 version.

In the spirit of continuous improvement, companies should periodically reassess their system of internal control over external financial reporting to identify opportunities to improve its efficiency and/or effectiveness. Leveraging COSO's 2013 Framework, which formalizes the principles embedded in the original more explicitly, incorporates business and operating environment changes over the past two decades, and improves the Framework's ease of use and application, is an effective way to do this.

The 2013 Framework also makes it easier for management to see what's covered and where gaps may exist in their current SOX 404 compliance program. For example, some companies may not have fully documented their internal control application in line with COSO's 1992 Framework. Others may have misinterpreted or misapplied the narrative in the original, thus falling short of an adequate assessment process with respect to one or more principles, or may have missed a principle outright. The

updated Framework develops principles and supporting points of focus within each of the five foundational components of internal control—control environment, risk assessment, control activities, information and communication, and monitoring activities. With it, management can more successfully diagnose issues and assert effectiveness regarding their internal controls and, for external financial reporting, help avoid material weaknesses or significant deficiencies. For all these reasons, I agree with the COSO Board's recommendation that users complete their transition "as soon as is feasible under their particular circumstances."

One Transition Approach

Considering that COSO's newly released Framework represents an update of the 1992 version and that the principles and requirements of effective internal control articulated in it were encompassed in the original, we expect a relatively smooth transition at Campbell Soup. Assuming we interpreted the original Framework properly in developing our current SOX compliance program, transitioning to the 2013 Framework by December 2014 may be limited to updating the format of several summary SOX reports. We don't expect a significant impact on our underlying SOX compliance methodology, approach, and/or key controls.

As co-lead of Campbell Soup Company's original global SOX team in 2003 and 2004, I played a key role in defining Campbell's SOX compliance methodology and approach. Like many companies, we selected the COSO *Internal Control—Integrated Framework* and then used it to assess the design and operating effectiveness of our internal controls over external financial reporting. We trained more than 300 cross-functional associates globally; designated operational and functional subteams to identify, document, and test Campbell's controls; and addressed deficiencies as needed.

Historically, Campbell Soup has consistently embraced the importance of maintaining a solid system of internal control. Thus, our primary challenge in 2003-2004 was to effectively document and test the controls already in place, including Campbell's control activities related to financial reporting as well as Campbell's company-level controls overall. To address company-level controls, we sifted through COSO's Framework and other guidance and then developed a customized template for Campbell Soup that consisted of key considerations or attributes for each of the five internal control components. Leveraging interviews with senior management and cross-functional experts as well as other evidence we collected, we documented the design and implementation and then assessed the operating effectiveness of these controls.

Even though we expect the transition from COSO's 1992 Framework to its 2013 Framework to result in few, if any, changes, we still need to work through it. The following five-step process represents one way to navigate the transition.

Table 1: Newly Released COSO Documents

Internal Control—Integrated Framework Executive Summary. Represents a high-level overview of the 2013 Framework and is intended for the CEO and other senior management, boards of directors, and regulators.

Internal Control—Integrated Framework and Appendices. This volume, approximately 175 pages, sets out the Framework in detail, defining internal control, describing the components of internal control and underlying principles, and providing direction for all levels of management in designing and implementing internal control and assessing its effectiveness. The appendices to this volume, including a glossary, specific considerations for smaller entities, summary of changes vs. the 1992 version, etc., provide additional reference but aren't considered part of the Framework.

Internal Control—Integrated Framework Illustrative Tools for Assessing Effectiveness of a System of Internal Control. This volume provides templates and scenarios to support management in applying the Framework, specifically in terms of assessing effectiveness.

Internal Control over External Financial Reporting: A Compendium of Approaches and Examples. This compendium provides practical approaches and examples illustrating how the components and principles set forth in the Framework can be applied in preparing external financial statements. It is intended to be used as a resource for questions and research on specific principles and components rather than being read from cover to cover.

STEP ONE: Develop Awareness, Expertise, and Alignment

In addition to gaining senior leadership alignment and support, the first step in transitioning to COSO's 2013 Framework is to build internal awareness and, ultimately, expertise among the resident COSO/SOX subject matter experts in your company. To do so, you and your team should obtain and review COSO's newly released publications, including the *Internal Control—Integrated Framework Executive Summary, Framework and Appendices, Illustrative Tools for Assessing Effectiveness of a System of Internal Control*, and the *Internal Control over External Financial Reporting (ICEFR): A Compendium of Approaches and Examples*. See Table 1 for a brief overview of each of these documents.

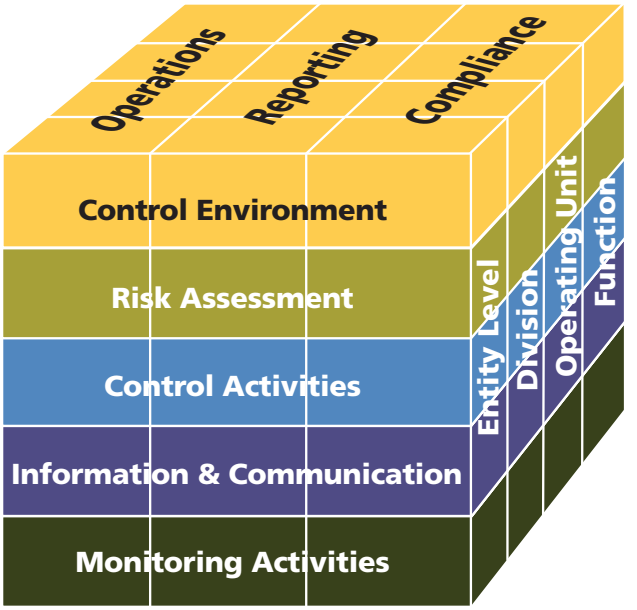
Combined, these COSO publications represent nearly 500 pages of guidance, so you may want to leverage other tools and resources as well. Here are some documents and other resources that will help you navigate the changes introduced in the 2013 Framework and its accompanying guidance. First, in addition to the *Executive Summary*, recent COSO press releases, a COSO presentation deck, "Frequently Asked Questions" document, and other materials are available on COSO's website (www.coso.org). They will provide an effective overview of COSO's Refresh Project in general and the 2013 Framework in particular.

Likewise, the five sponsoring organizations have been supporting COSO in building awareness of the updated Framework, so a review of their respective websites may provide additional insight and perspective. Several of them, as well as other parties, will be hosting a series of webinars and/or in-person seminars, forums, and/or training sessions, many of which will be available free to the public. Also, I'm sure numerous articles and editorials over the next year or so will offer various perspectives on applying the Framework, understanding key concepts in the Framework, and transitioning to it. Your external auditor, other public companies, regulatory authorities, and other relevant parties also can be great resources. Finally, networking and building connections with peers at similar companies can benefit you and your team.

As you begin developing your awareness, the following concepts and insights may be of particular interest:

Timeless Concepts. As noted earlier, COSO's key concepts regarding internal control are timeless. According to COSO, "Internal control is a process effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance." The 2013 Framework still provides for three categories of objectives—operations, reporting, and compliance—and still consists of five integrated components of internal control—control environment, risk assessment, control activities, information and communication, and monitoring activities. The Framework continues to be adaptable to a given organization's structure, allowing you to consider internal controls from an entity, divisional, operating unit, and/or functional level, such as for a shared services center. Finally, the important role of management judgment in designing, implementing, and maintaining internal control, as well as assessing its effectiveness, is retained. See Figure 1 for a visual representation of COSO's *Internal Control—Integrated Framework* (i.e., the updated COSO Cube).

Figure 1: The COSO Cube



Expanded Reporting Category. Whereas the reporting category of objectives was leveraged primarily for external financial reporting in the past, this category now explicitly and more clearly encompasses both internal and external financial and nonfinancial reporting objectives. COSO's Framework was always intended to address a broader spectrum of business activity, but the passage of SOX Section 404 resulted in a public perception that COSO could support external financial reporting only. The 2013 Framework now explicitly permits use in these other reporting situations, even though they aren't directly relevant from a SOX perspective.

Codified Principles. The 1992 Framework conceptually introduced 17 relevant principles associated with the

Table 2: 17 Principles

Here are the titles of the 17 internal control principles by internal control component as presented in COSO's 2013 Framework:

CONTROL ENVIRONMENT

1. Demonstrates commitment to integrity and ethical values
2. Exercises oversight responsibility
3. Establishes structure, authority, and responsibility
4. Demonstrates commitment to competence
5. Enforces accountability

RISK ASSESSMENT

6. Specifies suitable objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Identifies and analyzes significant change

CONTROL ACTIVITIES

10. Selects and develops control activities
11. Selects and develops general controls over technology
12. Deploys through policies and procedures

INFORMATION & COMMUNICATION

13. Uses relevant information
14. Communicates internally
15. Communicates externally

MONITORING

16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies

Please see the Framework for the actual principles and related descriptions.

five components of internal control. But these concepts were implicit in the narrative. Because they are essential in assessing that the five components are present and functioning, these concepts are now explicitly articulated in the 17 principles. The COSO Board believes each principle adds value, is suitable to all entities, and, therefore, is presumed relevant. If management determines that a given principle isn't relevant to the organization, it should document the rationalization. See Table 2 for a list of the principles and the associated components of internal control.

Table 3: Example Points of Focus

Principle 1. The organization demonstrates a commitment to integrity and ethical values.

Supporting Points of Focus:

- Sets the tone at the top
- Establishes standards of conduct
- Evaluates adherence to standards of conduct
- Addresses deviations in a timely manner

Requirements of Effective Internal Control. For management to conclude that its system of internal control is effective, all five components of internal control and all relevant principles must be present and functioning. Being "present" implies a given component or principle exists within the design and implementation of an entity's system of internal control. "Functioning" implies the component or principle continues to exist in the operation and conduct of the control system. Effective internal control also requires that all five components operate together in an integrated manner. Management can conclude they do if each component is present and functioning and the aggregation of internal control deficiencies across the components doesn't result in one or more major deficiencies.

Internal Control Deficiencies. According to the 2013 Framework, a major deficiency exists if an internal control deficiency or combination thereof severely reduces the likelihood of an entity achieving its objectives. In other words, if management used its professional judgment to determine that a control objective isn't being met because a relevant principle or associated component isn't present and functioning, or the five components aren't operating together, the entity has a major deficiency. Though the 2013 Framework uses and defines the terms deficiency and major deficiency, management should use relevant criteria as established by regulators, standards-setting bodies, and other relevant third parties for defining the severity of, evaluating, and reporting internal control deficiencies when reporting under those regulations or standards.

Points of Focus. COSO's updated Framework describes points of focus to assist management in designing, implementing, and maintaining internal control and in assessing whether the 17 principles are present and functioning. Points of focus represent important characteristics of the respective principles. (See Table 3 for

examples.) Points of focus deemed relevant and suitable for a given entity, whether described in the Framework or uniquely identified by management, can help you understand the respective principles. But management isn't required to separately assess whether they are in place. Points of focus are simply enablers; they aren't required in order to have an effective system of internal control.

STEP TWO: Conduct Preliminary Impact Assessment

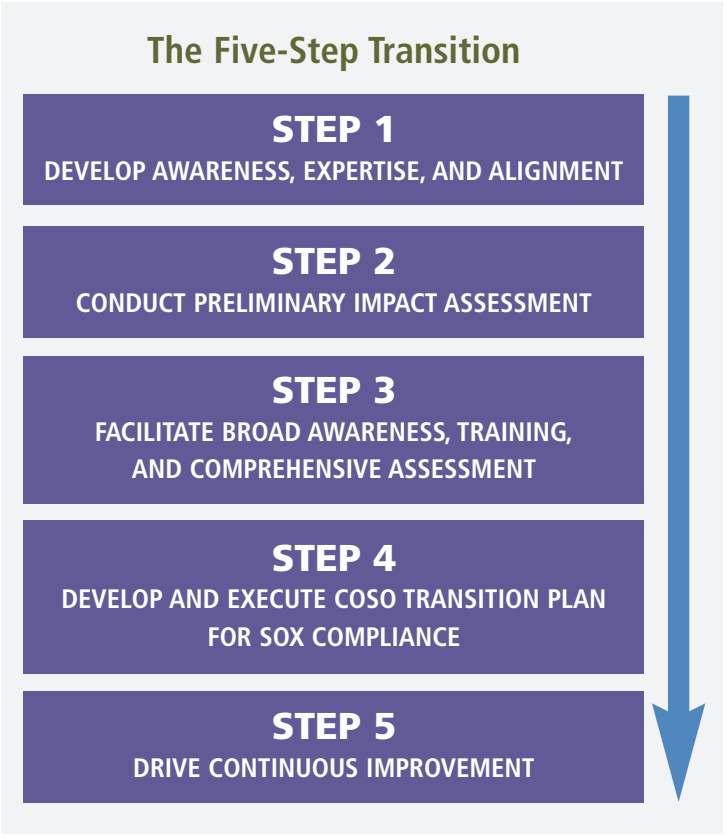
Once you understand COSO's 2013 Framework, you need to assess how transitioning to it will impact your current SOX compliance program. Perhaps the most significant factor affecting your transition from the 1992 version to the 2013 version is how well management implemented the original one.

To conduct a preliminary impact assessment, you should map your existing system of internal control against the updated COSO Framework. This will help you determine the degree of work required to complete the transition.

While developing your current methodology and approach for SOX compliance, you likely invested significant time up front to define your entity's internal control framework, starting with COSO's 1992 Framework and then customizing it based on your company's specific processes, financial disclosures, and risk history. Does the following scenario sound familiar?

First, management probably specified a high-level financial reporting objective and subobjectives related to preparing financial statements and disclosures. In doing so, it identified significant financial statement accounts based on the risk of material misstatement. Then, for each account or disclosure, management identified relevant financial reporting assertions, including existence, completeness, rights and obligations, valuation or allocation, presentation and disclosure, and the like. In addition, management identified underlying transactions, events, and processes supporting the respective accounts and disclosures. The result may have been a mapping of the design of your company's internal control environment, providing evidence that control activities are in place for all relevant financial reporting assertions for all significant accounts and disclosures. If there were any significant gaps, you remediated them accordingly.

Assuming you went through such a process in developing your existing SOX compliance program, you can leverage the original mapping to determine the impact of transitioning to COSO's 2013 Framework. Now, however, instead of mapping directly to the five components of internal control, you will first map to the 17 principles that underlie each of the five components. As before, if you determine there are gaps in your internal control design, you'll need to remediate them accordingly.



STEP THREE: Facilitate Broad Awareness, Training, and Comprehensive Assessment

In Steps One and Two, the effort was limited to the company's SOX compliance subject matter expert(s) and/or core SOX compliance team. Step Three entails engaging the broader organization to build awareness and to pressure-test the preliminary impact assessment conducted in Step Two.

Depending on the nature and complexity of your organization, your SOX compliance efforts may occur centrally, or there may be multiple layers of assessment. For example, each business unit or location may prepare its own local-level assessment. Either way, you should facilitate broad awareness of COSO's updated Framework and the potential impact on your SOX compliance program among key stakeholders, including the board of directors/audit committee, senior and operational management, process and control owners, and internal auditors. You should also discuss the impact of COSO's 2013 Framework on your SOX efforts with your company's external auditors. In some

cases, providing stakeholders a brief update, via memo or in person, will be sufficient. In other cases, in-depth training and work sessions may be needed.

In addition to building broad awareness, you should also leverage key stakeholders, such as process/control owners or business unit SOX leads, to pressure-test your preliminary impact assessment, especially in a more decentralized or highly complex environment. In other words, have those who are directly responsible for implementing your company's SOX controls critique the preliminary mapping from Step Two to ensure the analysis is complete and accurate.

STEP FOUR: Develop and Execute COSO Transition Plan for SOX Compliance

Once you've built broad awareness regarding the updated COSO Framework, gained senior leadership alignment and support that a timely transition is important, and completed a comprehensive impact assessment, it's time to develop and execute your company's transition plan. As with any well-managed project, the planning phase is usually the most important. During this phase, finalize your company's updated SOX compliance methodology and approach, define project governance and decision rights, develop a detailed project plan with key milestones, identify and assign resources, and complete other necessary planning activities. Most important, be realistic in your expectations and plans. Even those companies with sophisticated SOX compliance programs today who have designed, implemented, and maintain effective systems of internal control will have to expend some effort in the transition.

As you execute your transition plan, you will likely pass through three high-level phases:

Phase 1: Documentation and Evaluation. During this phase, you may need to update the format and/or flow of your underlying documentation, aligning it to the new mapping created during Step Two. Specifically, for management to conclude that its system of internal control is effective, all five components of internal control and all relevant principles must be present and functioning. The underlying documentation must support management in making such a conclusion. This phase also entails evaluating the design of the underlying controls and enhancing the design as needed.

Phase 2: Validation Testing and Gap Remediation. Once you're comfortable that your company's controls around external financial reporting and disclosure are effective in their design, you need to perform SOX validation testing to ensure these controls have been implemented and are operating as expected. If you identify deficiencies as a result of this testing, gap remediation may be required.

Phase 3: External Review and Testing. At some point, your external auditor will need to assess and gain comfort with your updated SOX compliance program and supporting documentation.

Impact of COSO's 2013 *Internal Control—Integrated Framework* on Prior COSO Documents

COSO's newly released 2013 *Internal Control—Integrated Framework* and related documents impact prior COSO publications as follows:

- COSO will consider the 1992 *Internal Control—Integrated Framework* as having been superseded by the 2013 Framework after 12/15/14.
- COSO will consider the 2006 *Internal Control over Financial Reporting—Guidance for Smaller Public Companies* as having been superseded by the ICEFR Compendium after 12/15/14.
- The COSO Board believes internal control is an integral part of enterprise risk management (ERM) but that ERM is broader in scope. As such, COSO's 2004 *Enterprise Risk Management—Integrated Framework* and the newly released *Internal Control—Integrated Framework* are considered complementary.
- COSO's 2009 *Internal Control—Integrated Framework, Guidance on Monitoring Internal Control Systems* will continue to be relevant and useful material for management.

STEP FIVE: Drive Continuous Improvement

In the true spirit of corporate governance, there's a difference between an adequate and a best-in-class system of internal controls. For a public company, stronger corporate governance should translate into stronger business results and increased shareowner value.

Once your company's transition to the 2013 Framework is complete, challenge yourself to drive continuous improvement thereafter with these practices:

Ensure there is appropriate tone at the top. Clearly communicate the company's commitment to

integrity and ethical values, the importance of maintaining effective internal control, and the expectation that all employees will fulfill their internal control obligations. Consider leveraging Web-based integrity programs to train employees on the company's standards of conduct and other important issues.

Embed internal control responsibility into the fabric of your company's culture, business processes, and procedures. One way to achieve this is to implement a control self-assessment (CSA) program as part of the company's ongoing evaluations within its monitoring activities component. CSA is a sustainable process whereby management periodically validates the operating effectiveness of the company's key controls vs. relying on internal or external auditors to make such an assessment. CSA drives management accountability and increases confidence in management's assessment of the effectiveness of their internal control system.

Leverage technology to support other monitoring activities. You can use technology solutions for comparing transaction details against predetermined thresholds, monitoring for trends and patterns, and assessing automated performance indicators and metrics.

Improve control reporting and communication. Consider developing dashboards related to key processes, activities, or controls that can alert you to potential anomalies or failures.

Enhance your enterprise risk management capability. Integrating your ERM process with your internal controls system will improve your company's ability to achieve its strategic, operational, reporting, and compliance objectives.

These are just a few examples of how you can drive continuous improvement of your company's system of internal control.

Call to Action

One last reminder: Those who currently use COSO's 1992 Framework should complete their transition to the 2013 version no later than December 15, 2014, at which time the original Framework will be considered superseded.

Now the onus is on me, you, and others within publicly traded companies subject to SOX Section 404 compliance to build awareness of the 2013 Framework, gain senior management's alignment and support, assess the impact of the Framework on existing SOX compliance activities, and then complete a timely transition. The five-step process outlined here is one approach that could support you and your team in doing so successfully. **SF**

J. Stephen McNally, CPA, is a finance director and controller for Campbell Soup Company. He has represented IMA on COSO's Internal Control—Integrated Framework Advisory Council since its inception in January 2011. In addition, he chairs IMA's COSO Advisory Panel and serves on IMA's Global Board of Directors. You can reach Steve at j_stephen_mcnally@att.net.

Supporting Subject Matter Experts

A special thank-you goes to the following individuals who shared their expertise and insight regarding the use of COSO's *Internal Controls—Integrated Framework* for SOX compliance and acted as a sounding board for the writing of this article:

Chet Davis, Campbell Soup Company, Chief Information Security Officer, Campbell Soup Company

Brian Ems, Campbell Soup Company, Director Financial Policy & Controls, Campbell Soup Company

Tania Herke, Springleaf Financial Services, Director Financial Policy

Stacy Juchno, PNC, SOX Director

David Landsittel, COSO Chair

Ray Purcell, Pfizer, Director of Financial Controls

Thomas Ray, Baruch College, City University of New York and former PCAOB Chief Auditor

Jennie Rothweiler, The Hershey Company, Global Internal Controls Compliance Manager

Bill Schneider, AT&T, Director of Accounting