Questions from Our Webinar

COSO 2013: What’s New, What’s Changed, Why Does It Matter and Other FAQs

Introduction

On September 11, 2013, Protiviti hosted a webinar to address the many questions and comments raised in the market in response to the release of COSO’s Internal Control – Integrated Framework (2013 edition). During the webcast, our audience of more than 1,300 executives and professionals submitted numerous questions – far more than we had time to address. Therefore, we are pleased to offer this supplement that provides detailed responses to many of the questions submitted.

For additional information, we invite you to download a complimentary copy of our resource guide, The Updated COSO Internal Control Framework: Frequently Asked Questions (Second Edition). Many of the questions below include references to relevant FAQs in this guide. You also are welcome to contact our COSO experts directly:

Jim DeLoach
Managing Director
+1.713.314.4981
jim.deloach@protiviti.com

Keith Kawashima
Managing Director
+1.408.808.3222
keith.kawashima@protiviti.com

Questions from the Audience

1. Specifically for SOX 404 compliance does Principle #6 (Risk Assessment) apply for only external financial reporting objectives or do the compliance and operations objectives also apply?

The SOX 404 assessment is focused solely on the external financial reporting objective. As such, the compliance and operations objectives do not apply. The compliance objective only applies to the extent that the organization is assessing its compliance with Section 404 of the Sarbanes-Oxley Act of 2002.

3. **What is the materiality role in the new framework? Was there any significant change from the old COSO to the new COSO in regard to the materiality concept?**

No, there is no change in regard to the materiality concept. Principle 6 addresses the specification of objectives with sufficient clarity and granularity to provide a context for risk assessment. The points of focus germane to that principle state that the measurement threshold for external financial reporting when applying the reasonable assurance criterion to the evaluation of the design and operating effectiveness of internal control is the conventional materiality standard.

**Protiviti COSO FAQ Guide:** See Question 8.

4. **The original COSO framework appeared to be geared primarily toward SOX. The new framework appears to provide a more broad-based compliance framework. Are you aware of other compliance initiatives that plan to embrace the COSO framework?**

The original COSO internal control framework was written 10 years before the Sarbanes-Oxley legislation was enacted. While COSO was formed in response to fraudulent financial reporting, the 1992 framework addressed the three objectives of operations, financial reporting and compliance, and COSO always intended the framework to be applied broadly. The 2013 New Framework has been updated to reflect the current business environment, contributing to the perception of a broader framework. A lot has happened over the last 20 years.

There are non-U.S. regulations similar to U.S. SOX where organizations use COSO as their assessment framework. Outside of ICEFR, we are not aware of regulators pushing its use.

**Protiviti COSO FAQ Guide:** See Question 3.

5. **Is the new framework intended to pull Operations and Compliance into our SOX 404 Compliance activities? Or is the new framework simply intended to help show how internal controls can be applied/implemented within Operations and Compliance?**

The new framework is not intended to broaden the application of Section 404 compliance to operations and other compliance objectives. It is an improvement and update to the existing relevant and useful 1992 framework. The new framework expanded explanations for the non-ICEFR objective categories in order to broaden the use of the framework for other internal control assurance activities. For example, many companies are providing sustainability reporting to the public; the COSO framework could be used to design and assess the internal controls around the generation of this non-financial external reporting information.

**Protiviti COSO FAQ Guide:** See Questions 4 through 7.

6. **What guidance does the framework provide in terms of controls over third-party providers, specifically with respect to IT? Example: What controls should be in place around outsourced IT infrastructures and support?**

COSO references the concept of outsourced business processes in several places in the framework and addresses information technology controls in numerous places, as IT is interwoven throughout the framework. COSO states that information obtained from outsourced service providers that manage business processes on behalf of the entity, and other external parties on whom the entity depends, is subject to the same internal control expectations. When outsourced service providers perform controls on behalf of the entity, the framework provides the following:

- Management retains responsibility for controls over outsourced activities.
• Outsourcing presents unique risks and often requires selecting and developing additional controls over the completeness, accuracy, and validity of information submitted to and received from the outsourced service provider. Accordingly, risk assessment should consider these risks.

• Control activities may need to be established to address the integrity of the information sent to and received from the outsourced service provider.

• Information requirements are developed by the organization and communicated to outside service providers and other similar external parties. Controls support the organization’s ability to rely on such information, including internal control over outsourced service providers such as vendor due diligence, exercise of right-to-audit clauses, and obtaining an independent assessment over the service provider’s controls.

• The blurred lines of responsibility between the entity’s internal control system and that of outsourced service providers creates a need for more rigorous controls over communication between the parties.

• Monitoring applies to outsourced service providers. To that end, the framework provides specific guidance to consider.


7. Please provide clarity if companies are expected to transition to the new COSO framework effective Jan 1, 2014 to ensure compliance with SOX 302 requirements.

This is a legal question and companies are advised to consult with their counsel. It has been a longstanding practice that the Section 302 ICFR assessment be based on the most recent Section 404 assessment. The SEC has made it clear that Section 302 doesn’t require an update of that assessment, as implied by the “based on the most recent evaluation of internal control over financial reporting” language relating to disclosure of significant deficiencies, material weaknesses and fraud. The only exception would be the consideration of the effect of changes in ICFR to ascertain their significance for disclosure purposes.

The intent of the COSO Board in issuing its guidance was to provide a reasonable transition period so as to not cause undue hardship for companies during the transition period. COSO encouraged companies to transition to the 2013 New Framework as soon as they could, but recognized that for many companies the transition may take some time to complete. Our view is that the transition deadline of December 15, 2014 is literal, meaning there wasn’t any intent to require implementation of the 2013 New Framework beginning in the first quarter of 2014. The 1992 framework is still sound during the first quarter of 2014, as indicated in the COSO Board’s letter. The Section 404 assessment is an “as of” assessment as of end of year and the tests to validate design/operating effectiveness are substantially the same under the 1992 or 2013 versions of the COSO internal control framework.

Protiviti COSO FAQ Guide: See Question 16.

8. Is COSO 2013 required by law like SOX or will management view this as best practice?

COSO is not a regulator and cannot mandate the use of its framework. In conducting a Section 404 evaluation of ICFR, the SEC mandates the use of a “suitable framework.” The COSO Internal Control – Integrated Framework is an example of a “suitable framework.”

9. Does the movement of Information & Communication increase the focus and reliance on IT- and IS-related controls?

The updated framework has increased the focus on how technology is being used to implement internal controls. In practice, organizations have been assessing IT internal controls using frameworks such as COBIT for a number of years. As the technology environment has changed radically since 1992, COSO has updated the framework accordingly.


10. Is the ERM framework an acceptable model for internal control reporting for SEC-reporting organizations?

While the ERM framework deals with alternative risk responses (risk avoidance, acceptance, sharing and reduction), the internal control framework deals primarily with risk reduction. ERM focuses on strategic objectives and strategy setting and internal control does not, because achievement of strategic objectives is subject to external events not always within the organization’s control. The concepts of focusing on a portfolio view of risk and aggregating the effect of risk responses across the organization are not contemplated in the internal control framework. For these and other reasons, the COSO Internal Control – Integrated Framework is the preferred model for evaluating the effectiveness of ICFR.


11. One of the key message points in the new framework is that it can be used and applicable to all size entities, including non-profits, smaller companies, etc. All 17 principles need to be present and functioning for these "smaller", non-public entities as well, right? I get the sense that entities may try and argue that since they are not in a SOX environment (i.e., Public Entity) not all of the 17 principles need to be present and functioning. What kind of guidance can you give here?

12. Do COSO and the updated version for 2013 apply to public colleges?

13. The OCC is placing increased emphasis on Operational Risk Tests. Is COSO a viable approach?

The COSO framework is written to be used in any type of organization, public or private, for the design, implementation and assessment of internal control. It provides a disciplined approach to designing and assessing internal control, and can benefit all types of organizations. When using the framework to design, implement and assess internal controls around any of the three objective categories, there is a presumption that all 17 principles should be in place. Many smaller entities, however, find it very difficult to attract independent directors with the desired skills and experience. Typical challenges to finding suitable directors include inadequate knowledge of the entity and its people, the entity’s limited ability to provide compensation commensurate with board responsibilities, a sense that the chief executive might be unaccustomed or unwilling to share governance responsibilities appropriately, or concerns about potential personal liability. That limitation does not eliminate the importance of Principle 2 to internal control.

The COSO 2013 New Framework is designed to be applied in many circumstances, including public colleges. See Question 38 of our FAQs publication for the applicability of the COSO 17 Principles to other areas of compliance, including OCC requirements.

Protiviti COSO FAQ Guide: See Questions 6, 7 and 38.

The terminology of “present and functioning” and “operating together” versus “design effectiveness and operating effectiveness” illustrates COSO’s focus on providing a global framework that uses terminology that reaches across country borders and regulatory regimes. During our webinar, we contrasted the COSO terminology with the “design effectiveness and operating effectiveness” terms to make the 2013 New Framework relevant to the U.S. SOX environment.


15. From a SOX perspective when we do the mapping to the 17 principles do we limit it mainly to financial reporting objectives?

Yes.

Protiviti COSO FAQ Guide: See Question 17.

16. Is there going to be new guidance released for smaller companies?

17. Will guidance be provided for small companies?

The ICEFR Compendium provides additional relevant guidance that small companies can leverage, and Appendix C to the 2013 New Framework provides considerations for smaller entities. COSO previously issued small company guidance in 2006, Guidance on Internal Control over Financial Reporting - Guidance for Smaller Public Companies, which will be superseded when the original framework sunsets.

Protiviti COSO FAQ Guide: See Question 36.

18. Are there defined documentation requirements to validate that the 17 principles are in place and functioning?


COSO’s Illustrative Tools for Assessing Effectiveness of a System of Internal Control provides example templates for how to analyze the presence and functioning of the five components and 17 principles. You can purchase that publication from COSO.

Effective internal control will look different in each organization. Evaluation requires judgment and experience and cannot be prescriptive. The points of focus for the principles add substance and rigor to them.

Protiviti COSO FAQ Guide: See Question 33.

20. Where can we get access to the PCAOB findings?

Inspection reports on the public accounting firms are available on the PCAOB website at http://pcaobus.org/Inspections/Reports/Pages/default.aspx.

21. Should management and internal audit independently or jointly perform the mapping evaluation to principles?

Whoever is responsible for executing management’s assessment work for SOX should complete the mapping. In some organizations, this is a separate internal controls group. In others, it is internal audit working in conjunction with management. Once the mapping is complete, if another group completed the
mapping, internal audit could review this work and provide assurance regarding its completeness and sufficiency.

**Protiviti COSO FAQ Guide:** See Question 22.

**22. If there are weaknesses with the Control Environment, is there any point in continuing to evaluate the other components?**

No doubt, deficiencies in the Control Environment are a problem. In such situations, management’s focus should be on assessing these deficiencies in order to determine their magnitude and taking appropriate actions to remediate those gaps. For the same reason, the other components should be evaluated to ascertain whether deficiencies exist in those components requiring remediation. All five components must be evaluated to support management’s assertion.

**Protiviti COSO FAQ Guide:** See Questions 9 and 18.

**23. Whom do you consider "management" in your meet with management to discuss COSO 2013?**

We are referring to the certifying officers who sign the issuer’s internal control report, specifically the CEO and CFO. These two executives and the audit committee need to understand the ramifications of the 2013 New Framework on the issuer’s approach to Section 404 compliance.

**Protiviti COSO FAQ Guide:** See Question 27.

**24. Is there prescribed guidance on how to disclose which framework was used in the SOX internal control report?**

**25. Do we have to disclose which framework was used for the 2013 financial statements?**

**26. Is the required disclosure of which framework was used (old vs. revised) required for year-ending Dec 31, 2013?**

Yes. Where the framework is referenced in your SOX internal control report during the transition period, it would be appropriate to parenthetically reference the framework used. For example: “COSO Internal Control – Integrated Framework (1992) or (2013).” Since 2013 is during the transition period, when management issues its assertion on the effectiveness of ICFR for SOX Section 404 purposes and references the COSO framework, the version used should be referenced.

**Protiviti COSO FAQ Guide:** See Questions 20 and 29.

**27. What is expected to be the average time/effort to transition to the new framework?**

**28. Do you have any estimate on the transition effort (e.g., as a % of the current effort)?**

The level of effort will greatly vary based on the size of the organization, how well it updated its controls documentation to reflect changes in the organization, and whether the company applied COSO’s Small Company guidance when implementing the framework. The reality is that not many companies have adopted the framework since its release in May, so there isn’t an adequate base of experience to draw conclusions at this time. Therefore, it is important to begin the planning process soon if you haven’t done so already.

**Protiviti COSO FAQ Guide:** See Question 31.
29. Just to confirm, the SOX definition of deficiency is not the same as the COSO definition of deficiency. Can you specifically explain the difference?

30. Does a "major deficiency" imply a SOX 404 material weakness that precludes an unqualified opinion?

Correct.

The New Framework states that a deficiency is “a shortcoming in a component or components and relevant principle(s) that reduces the likelihood that the entity can achieve its objectives.” It is important to recognize that not every deficiency will result in a conclusion that an entity does not have an effective system of internal control. When an organization determines that a deficiency exists, management must assess the severity of impact of that deficiency on the internal control system. A major deficiency in internal control is defined as “an internal control deficiency or combination of deficiencies that severely reduces the likelihood that the entity can achieve its objectives.” Such a deficiency exists when management determines that a component (and one or more relevant principles) is not present or functioning or that the components are not operating together. The existence of a major deficiency prevents the organization from concluding that the system of internal control is effective.

When using the COSO framework for regulatory purposes, organizations should refer to the regulator’s criteria as the standard to use. The criteria in the U.S. for ICFR embodies the standard “deficiency, significant deficiency and material weakness” terminology that has been in place for several decades. This terminology will continue to be used for purposes of Section 404 compliance. Within that framework, a “control deficiency” exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. This definition is focused on misstatements, whereas the COSO definition is focused on achievement of objectives, e.g., reliable financial reporting. Needless to say, they are very much related as they cover the same thing in different ways.

Because the components being present and functioning are a primary focal point in reviewing the effectiveness of ICFR, a major deficiency under COSO would most likely translate to a material weakness for SOX.

Protiviti COSO FAQ Guide: See Question 18.

31. Should we adjust our Risk and Control Matrix to reflect the 17 principles or can they be addressed only at ELC level?

COSO supports a top-down, risk-based approach to assessing internal controls. When mapping principles to controls, start from the top and map to where the controls reside in your organization’s control structure.

There are a variety of ways to map principles to controls. Adjusting the RCMs may be one approach. It may also be possible to map principles to controls without adjusting the RCMs particularly if they delineate control activities and monitoring activities. It is our view that much of the documentation around Control Activities for SOX purposes would not change in format and the related financial reporting assertions will still be considered, linked to significant financial reporting elements (accounts and disclosures).

Protiviti COSO FAQ Guide: See Question 22.
32. I would like to see a model project plan for COSO 2013 implementation.

So would everyone else. Not many companies have adopted the framework since its release in May. We are working with companies in formulating their customized plans. While all plans vary from company to company, following is a high-level outline:

- Conduct internal discussion, present overview of framework to certifying officers and audit committee, summarize the key changes to existing approach, determine the mapping approach using the 17 principles, identify the relevant points of focus for each principle (assuming points of focus will be used), provide training to everyone who needs it, set a high-level time line and identify the necessary resources

- Conduct initial discussion with external audit firm to get their views on approach and issues, determine their expectations on changes in documentation, understand the key changes they see related to the company’s previous approach and identify areas that could be more difficult and require attention to address specific challenges

- Create 17 principles documentation inventory using an appropriate spreadsheet application, an automated software conversion module or some other tool
  - Create document that lays out the 17 principles – under each principle summarize at a high level “what the company has that demonstrates this principle is present and functioning”
  - Come to an initial conclusion, e.g., we have it nailed, we are in pretty good shape with some refinements needed, we have some controls that are relevant but have work to do to complete, or we must start from scratch
  - Use this perspective to plan the mapping exercise

- Map controls to principles and come to a preliminary conclusion regarding whether (1) the design of the documented controls is effective and (2) if the controls are determined to be operating effectively, would they allow management to conclude that the Principle is “present and functioning”
  - Determine controls that must be re-configured, changed, added/deleted for 2014, if any, to support a positive assertion in the internal control report

- Based on the above, finalize the action plan for 2014 to improve the control structure and test the operating effectiveness of controls and arrange for the necessary resources

- Meet with the external audit firm and present results of work, identified areas for revision, remaining action plan, etc.

- Execute remaining steps in the action plan and monitor progress to completion

Protiviti COSO FAQ Guide: See Question 33.

33. Can you describe some of the documentation that will need updating, besides some of our SOX documentation?

SOX ICEFR certification varies across issuers. Examples of SOX documentation likely to be impacted by the 17 principles:

- Evidence that the five components of the COSO New Framework are addressed;
- Results of management’s evaluation of controls design effectiveness;
- Results of management’s tests of controls operating effectiveness.
An overall high-level document might be prepared to evidence management’s assessment process. The SEC’s interpretive guidance provides the following example:

> [M]anagement may document its overall strategy in a comprehensive memorandum that establishes the evaluation approach, the evaluation procedures, the basis for management’s conclusions about the effectiveness of controls related to the financial reporting elements and the entity-level and other pervasive elements that are important to management’s assessment of [internal control over financial reporting]. If management determines the evidential matter within the company’s books and records is sufficient to provide reasonable support for its assessment, it may determine that it is not necessary to maintain copies separately of the evidence it evaluates.

This memorandum should describe the steps of the process and refer to the project documents and work products. It might list by Principle the number of key controls, the number of controls deemed “effective” and “ineffective” based on the initial testing, the number of “ineffective” controls remediated and retested, the number of controls for which a preliminary conclusion was reached requiring refresh testing, the controls for which refresh testing is completed, and the final conclusions.

To the extent the organization uses the COSO framework to design and/or evaluate internal controls around a different business objective (such as sustainability reporting, compliance with a particular regulation, etc.), the evaluation team would need to review the related documentation for gaps against the 17 principles.

34. Can you provide a simple example of what the control documentation would look like pre-conversion versus converted documentation?

35. Can you provide an illustrative example(s) of how 404 documentation would change under the new framework?

36. Do you have templates to use for early adoption now?

COSO’s Illustrative Tools for Assessing Effectiveness of a System of Internal Control provides example templates for how to analyze the presence and functioning of the five components and 17 principles. You can purchase that from COSO.

We do not have an example to share generically at this time, as most companies have not adopted the framework yet and we are not convinced a one-size-fits-all approach is the answer. That said, we would expect to see a mapping of the 17 principles to the relevant controls that the organization has previously documented, along with conclusions on the design and operation of the controls against those principles. In addition, we believe that much of the documentation around control activities for SOX purposes would not change in format and the related financial reporting assertions will still be considered linked to significant financial reporting elements (accounts and disclosures).
37. Any implications whatsoever on JSOX reporting for private companies?

38. What differences does the 2013 U.S. COSO framework have compared to the Japanese COSO framework?

If the COSO internal control framework is used as a suitable framework for JSOX compliance reporting for an organization, then management will need to go through a gap analysis as described in the webinar.

To our knowledge, there isn’t a “Japanese COSO framework.” There are many similarities between JSOX and Section 404. There are also differences. As noted above, the COSO framework can work in a JSOX environment.

39. Any change in organization regarding the 2\textsuperscript{nd} line of defense?

No, the COSO 2013 New Framework does not alter any of the various lines-of-defense models that people use.

Protiviti COSO FAQ Guide: See Question 22.

40. Is there a mapping between COSO 2013 and COBIT?

Many of COBIT’s objectives are at the control activities level and do not relate to the Control Environment, Risk Assessment or Monitoring Activities components of COSO. Since the COSO 2013 framework has only been out for about four months, many organizations have not gotten very far in comparing the two frameworks.


41. Are there any automated tools that will facilitate the documentation of risk and controls identified?

We expect software tools to evolve as organizations look for tools to help them map their controls to the 17 principles. For example, Protiviti is updating the SOX modules of its Governance Portal to enable the mapping of the principles to the control register. The release date is TBD.

42. What are the changes we should implement in our risk-based audit approach?

43. Does our internal audit analysis methodology have to change due to the new framework?

44. How will the new COSO impact internal audit work?

If you have adopted COSO Internal Control – Integrated Framework for your internal audit function and, in particular, state this in your charter, you will want to assess your methodology to determine if there are any gaps in your approach around planning, execution and reporting. Many of the principles in the 2013 New Framework are implicit in many internal audit methodologies. To the extent that your internal audit function provides any overall opinions and uses the COSO framework as the standard for the scope of work and opinion, the audit methodology would need to be assessed to determine what might need modification. COSO is not mandated by The IIA. However, as a sponsoring organization of COSO, The IIA would likely strongly encourage its adoption by internal audit functions.

Protiviti COSO FAQ Guide: See Questions 6 and 22.
45. Do you expect more updates/changes to the proposal thus should we wait until 2014 for transition?

46. Will this be delayed further?

The 2013 COSO Internal Control – Integrated Framework is final, and was subject to a rigorous public comment process. We do not expect that any further changes will be made to it as COSO exposed it to the public twice. We also do not anticipate any extension to the transition period. Accordingly, organizations should proceed with their implementation to meet the December 2014 deadline.


47. Is an IT Governance review required as part of the COSO control framework implementation?

48. I want to learn how much emphasis will be placed on IT under the new framework.

COSO outlines a description of technology general controls to include control activities over the technology infrastructure, security management, and technology acquisition, development, and maintenance (Principle 11). IT application controls are embedded in the processes with other control activities and are implicit in Principles 10 and 12. Thus, aspects of IT governance are implicit in the framework. Most companies have already documented and tested these processes for their ICEFR SOX process. COSO essentially is updating its internal control framework to address the reality that companies have already been evaluating these types of controls. Having said that, COSO is not prescriptive in its guidance. Individuals looking for specifics will need to consult other resources, such as COBIT.


49. Are there any books or guidance outside of COSO that would assist?

50. What resources are available to help me know how to implement?

The COSO 2013 New Framework is your best bet. In addition, there are the illustrative templates and ICEFR compendium that accompany the Framework.


The IIA is offering training on the framework, FEI has been holding roundtables, and The IIA has published a book. The external audit firms continue to issue briefs on the topic, and we should expect to hear more from them into early 2014.

Protiviti COSO FAQ Guide: See Question 33.

51. Is Protiviti going to modify their software to accommodate COSO 2013 versus the old COSO 1992 standard?

Yes, Protiviti is in the process of updating its Governance Portal to provide approaches for existing users to map their controls inventory to the 17 principles. This will include reporting capability to summarize results to enable the process. We hope to have a release date available for our October 30 webinar.
52. Will accounting firms need to provide their assessment based on the new framework?

The external auditor has to use the same framework as management. So when management transitions, the external auditor will have to transition as well.


53. Will a site license version be available so that large institutions can train multiple personnel?

You can purchase a license from COSO for a discrete number of seats to the full framework.

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. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE 1000® and FORTUNE Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

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.

About Our Financial Controls and Sarbanes-Oxley Compliance Practice

Protiviti’s Financial Controls and Sarbanes-Oxley Compliance professionals help companies establish effective internal control over financial reporting. Whether your organization is just getting started or has complied for years, we help companies apply a top-down, risk-based approach, in accordance with the U.S. SEC’s interpretive guidance, to implement a cost-effective compliance process. We help rationalize the critical risks, identify the key controls, develop a credible body of evidence supporting controls design and operating effectiveness, drive accountability for compliance throughout the organization, and coordinate the optimization of the attestation process under Auditing Standard No. 5.

Our experience, gained by working with hundreds of companies, gives us the knowledge to help organizations think longer-term, make the right choices and create value as sustainability improves. Our flexible, comprehensive approach is driven by a customized road map that addresses each client’s immediate priorities, planned improvements, longer-term strategic improvements and designated timetable.

Our specific services include:

- Sarbanes-Oxley compliance project planning and management
- Documentation, evaluation, testing and remediation of risks and controls
- Compliance cost reduction by rationalizing risks and controls and implementing risk-based testing
- Improvement of internal controls and the quality of key upstream business processes affecting financial reporting
- Governance portal implementation and support

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.