The Updated COSO Internal Control Framework

Frequently Asked Questions

Third Edition

protiviti®
Risk & Business Consulting.
Internal Audit.

Powerful Insights. Proven Delivery.®

Introduction

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) – an organization providing thought leadership and guidance on internal control, enterprise risk management (ERM) and fraud deterrence – released its long-awaited updated *Internal Control – Integrated Framework* (New Framework) in May of 2013. The original version (framework), released by COSO in 1992, has gained broad acceptance. It has been widely used, particularly as a suitable – and the predominant – framework in conjunction with reporting on the effectiveness of internal control over financial reporting (ICFR) by public companies listed in the United States in accordance with Section 404 of the Sarbanes-Oxley Act. It is also commonly used for other similar regulatory requirements outside the United States, such as the Japanese equivalent of Section 404 (often referred to as "JSOX"). Today, this time-tested framework continues to be recognized as a leading resource for purposes of providing guidance on the design and evaluation of internal control. While companies will likely continue to use the COSO framework for reporting on their financial reporting controls, they also can apply it in assessing internal control over operations, compliance and other reporting objectives.

The New Framework issued by COSO is an important development, as it facilitates efforts by organizations to develop cost-effective systems of internal control to achieve important business objectives and sustain and improve performance. It also supports organizations as they adapt to the increasing complexity and pace of a changing business environment, manage risks to acceptable levels and improve the reliability of information for decision-making. Companies using the 1992 framework for Sarbanes-Oxley compliance and other purposes should familiarize themselves with the New Framework and companion materials, determine their transition plan, and communicate to the appropriate stakeholders the release of the New Framework and its implications to the organization. It is hoped that this guide will help them as they execute their transition plans.[1]

This third edition of our guide addresses various questions regarding the New Framework from COSO, including the reasons why it was updated; what has changed; the process for transitioning to its use; and steps companies should take now. It has been updated with additional questions that have arisen since publication of the second edition, particularly from discussions with clients and webinars we have conducted. For interested parties, the New Framework is available at www.coso.org.

Protiviti

April 2014

[1] For further guidance, refer to our *Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements – Frequently Asked Questions Regarding Section 404* (Fourth Edition), available at http://www.protiviti.com/en-US/Pages/SOX-404-FAQs.aspx and our *Guide to the Sarbanes Oxley Act: IT Risks and Controls* (Second Edition), available at http://www.protiviti.com/en-US/Pages/Guide-to-the-Sarbanes-Oxley-Act.aspx.

Table of Contents

* Indicates new or revised material (compared to the second edition of this resource guide)

* Indicates new or revised material (compared to the second edition of this resource guide)

* Indicates new or revised material (compared to the second edition of this resource guide)

1. Who is COSO?

The Committee of Sponsoring Organizations of the Treadway Commission was organized in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private-sector initiative that studied the causal factors that can lead to fraudulent financial reporting. It also developed recommendations for public companies and their independent auditors, for the U.S. Securities and Exchange Commission (SEC) and other regulators, and for educational institutions. It is sponsored jointly by five major professional associations headquartered in the United States: the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), The Institute of Internal Auditors (IIA), and the Institute of Management Accountants (IMA).

2. How did the project to update the 1992 framework unfold?

In 2010, COSO decided to update the 1992 framework with a fresh look and engaged PricewaterhouseCoopers (PwC) to do the project. An Advisory Council was formed consisting of representatives from industry, academia, government agencies and not-for-profit organizations to provide input as the project progressed. Protiviti had a representative on the Advisory Council. Exposure drafts were issued to the public for comment and COSO received feedback in the form of responses to an online survey as well as public comment letters. Based on this input, COSO finalized the update, resulting in the New Framework.

3. How is the updated framework organized?

Developed and authored by PwC under the direction of the COSO Board over a two-and-a-half year period, the New Framework and related illustrative documents consist of an executive summary, the New Framework itself, several appendices,[2] an applications guide providing illustrative tools, and a separate compendium of approaches and examples for application of the New Framework to ICFR.

4. Why update the 1992 framework?

"If it ain't broke, don't fix it." This old saying begs a question regarding the 1992 framework: Was it broken? In a word: No. In the spirit of continuous improvement, COSO's decision to update the framework was driven by the extent of change over the past two decades. Much has happened in the business environment since 1992. For example, expectations for governance oversight have increased; risk and risk-based approaches now receive greater attention; globalization of markets and operations has become a mega trend; the complexity of business and organizational structures has increased, including outsourcing and strategic suppliers; technology has evolved dramatically; and the demands and complexities in laws, regulations and standards have all increased – substantially.

We also have seen the damaging effects of spectacular, large-scale governance and internal control breakdowns, including the derivatives fiascoes of the 1990s, Long-Term Capital Management, the Enron era, and the more recent global financial crisis. These breakdowns have taught valuable lessons around a number of themes – for example, the effects of management override, conflicts of interest, lack of segregation of duties, poor or nonexistent transparency, siloed risk management, ineffective board oversight, and unbalanced compensation structures that enabled or drove dysfunctional and/or irresponsible behavior.

While no internal control framework provides answers to all of these issues, there is no denying that much has transpired since COSO's 1992 framework was issued, and it makes sense for it to be updated in light of those changes. Add to the above developments the increased expectations for competencies and accountabilities at all levels of organizations, and the heightened expectations around preventing and detecting fraud, and you've got a viable business case for a refresh of a 20-year-old framework.

---

[2] The appendices include a glossary of key terms, a summary of roles and responsibilities, a discussion of the process used to update the framework, a discussion of the comment letters received, a summary of changes to the 1992 framework, and a comparison of the New Framework with COSO's Enterprise Risk Management – Integrated Framework.

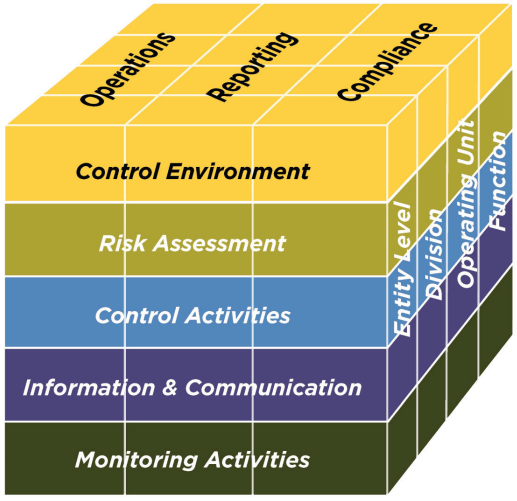
5. What hasn't changed?

Those experienced at using the 1992 version will find much familiar in the 2013 New Framework, as it builds on what has proven effective in the original release. For example, the New Framework retains the core definition of internal control and the five components of internal control that provide the face of the well-known, three-dimensional "cube." We discuss further below.

The core definition of internal control is largely unchanged. The updated definition reflects the expansion of the reporting objective (discussed later):

> 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 cube retains its familiarity. It begins with objectives along the top relating to operations, reporting and compliance, representing the cube's columns. Every organization establishes relevant objectives and formulates strategies and plans for achieving them. The side of the cube, as shown below, depicts that objectives may be set for the entity as a whole, or be targeted to specific divisions, operating units and functions within the entity (including business processes such as sales, purchasing and production), illustrating the hierarchical top-down structure of most organizations.



Source: Chapter 2 of the 2013 COSO *Internal Control: Integrated Framework.*

On the face of the cube are the five components of internal control, representing the rows of the cube. Similar to the 1992 framework, these components support the organization in its efforts to achieve its objectives. The five components are Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities. They are relevant to an entire entity, meaning they operate at the entity level, as well as at all divisions, operating units, functions, subsidiaries or other subsets of the entity.

All told, the cube depicts the direct relationship among the organization's objectives (which are what the entity strives to achieve); the components of internal control (which represent what is needed to achieve the objectives); and the operating units, legal entities and other structures within the entity (which are the levels of the organization where the components of internal control operate). Each internal control component cuts across and applies to all three categories of objectives.

With the definition of internal control and the structure of the cube and its dimensions fundamentally the same as the original 1992 version, ***the criteria used to assess the effectiveness of an internal control system remain largely unchanged.*** The effectiveness of internal control is assessed, using a principles-based approach, relative to the five components of internal control. To have an effective system of internal control relating to one, two or

more categories of objectives, all five components must be present and functioning and operating together. For example, when considering internal control over a particular operations objective, all five components must be present and functioning and operating together in order to conclude that internal control relating to the operations objective is effective.

The other aspect of the New Framework that is unchanged is the exercise of judgment. The New Framework continues to emphasize the importance of management's judgment in evaluating the effectiveness of a system of internal control. Determining whether a particular internal control system is effective is a subjective judgment resulting from an assessment of whether each of the five components of internal control is *present and functioning*, and that the five components of internal control *operate together* to provide "reasonable assurance" the relevant objectives are met. To facilitate this exercise of judgment, principles are provided for each internal control component and management exercises judgment in determining the extent to which these principles are *present and functioning*.

6. What has changed?

The New Framework has several important changes. Seven are discussed below:

First, the New Framework codifies principles that support the five components of internal control. While the 1992 version implicitly reflected the core principles of internal control, the 2013 version explicitly states 17 principles representing fundamental concepts associated with the five components of internal control.[3] COSO decided to make these principles explicit to increase management's understanding as to what constitutes effective internal control. These principles remain broad, as they are intended to apply to for-profit companies (including publicly traded and privately held companies), not-for-profit entities, government bodies and other organizations.

Supporting each principle are points of focus, representing important characteristics associated with the principles. Points of focus are intended to provide helpful guidance to assist management in designing, implementing and conducting internal control and in assessing whether relevant principles are present and functioning; however, while the New Framework defines 77 points of focus, it does not require separate evaluations of whether all 77 are in place. Management has the latitude to exercise judgment in determining the suitability or relevancy of the points of focus provided in the New Framework. In fact, the New Framework allows for and supports the possibility that management may identify and consider other important characteristics germane to a particular principle based on the organization's specific circumstances.

Together, the components and principles constitute the criteria, and the points of focus provide guidance that will assist management in assessing whether the components of internal control are present, functioning and operating together within the organization. Each of the points of focus is mapped directly to one of the 17 principles, and each of those principles is mapped directly to one of the five components.

Second, the New Framework clarifies the role of objective-setting in internal control. The 1992 framework from COSO stated that objective-setting was a management process, and that having objectives was a pre-condition to internal control. While the New Framework preserves that conceptual view, it moves the primary discussion of the concept from the chapter on risk assessment to the second chapter to emphasize the point that objective-setting is not part of internal control.

Third, the New Framework reflects the increased relevance of technology. This is important because the number of organizations that use or rely on technology, and the extent of that use, have both grown substantially over the past 20 years. Technologies have evolved from large stand-alone mainframe environments that process batches of transactions to highly sophisticated, decentralized and mobile applications involving multiple real-time activities that cut across myriad systems, organizations and processes. More sophisticated technology can impact how all components of internal control are implemented.

---

[3] This is not a new concept for COSO. A principles-based approach was undertaken by COSO in its 2006 release of *Internal Control over Financial Reporting — Guidance for Smaller Public Companies*. The idea is to use principles to enhance the understanding of, and simplify, the internal control design and evaluation process.

Fourth, the New Framework incorporates an enhanced discussion of governance concepts. These concepts relate primarily to the board of directors, as well as subcommittees of the board, including audit committees, compensation committees and governance committees. The key message is that board oversight is vital to effective internal control.

Fifth, as evidenced through being the primary visual change in the cube, the New Framework expands the reporting category of objectives. The financial reporting objective category is expanded to consider other external reporting beyond financial reporting,[4] as well as internal reporting, both financial and non-financial. Thus, there are four types of reporting – internal financial, internal non-financial, external financial and external non-financial.

Sixth, the New Framework enhances consideration of anti-fraud expectations. The 1992 framework considered fraud, although the discussion of anti-fraud expectations and the relationship between fraud and internal control were less prominent. The 2013 version contains considerably more discussion on fraud and also considers the potential causes of fraud as a separate principle of internal control.

Finally, the New Framework increases the focus on non-financial reporting objectives. This expanded focus on operations, compliance and non-financial reporting objectives has resulted in more robust guidance in these areas. This guidance is provided in hopes that more users will apply the New Framework beyond financial reporting.

The above changes, while important, in no way constitute a complete overhaul. Those individuals familiar with the 1992 framework will find the New Framework to be similar in substance in all material respects.

7. What's the most important change?

The most significant change in the New Framework is the explicit articulation of the 17 principles representing the fundamental concepts associated with each component of internal control. Because these principles are drawn directly from the components, an entity can achieve effective internal control by applying all of them. All of the principles apply to each category of objectives, with the intent of making the New Framework more principles-based.

The use of principles is not meant to imply a checklist. This was a major concern raised in comments on the exposure drafts circulated by COSO, particularly with respect to the points of focus related to each principle. In using the principles to assess whether the system of internal control is effective, management and the board of directors determine the extent to which the principles associated with each of the five components are present and functioning. This evaluation entails consideration of how the principles (and the underlying points of focus, if considered) are being applied.

Five components of internal control are about as broad as you can get. The 1992 version explained each component, and the supporting application guidance incorporated much of the explanatory material into the various evaluation tools that users of the original framework leveraged to design their own customized tools. The New Framework now organizes explanatory material under the 17 principles arrayed under the five components. While people can call it what they want, the desired end result is to help users better understand what constitutes effective internal control so they are positioned to apply informed judgment when evaluating effectiveness.

To illustrate, the 17 principles are listed below and grouped according to the applicable COSO component:

Control Environment

1. The organization demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

[4] The internal control report issued under Section 404(a) of the Sarbanes-Oxley Act in the United States is an example of "other external reporting." Another example might include where management operates in accordance with the International Organization for Standardization (ISO) standards for quality management. In such instances, it may report publicly on its operations (e.g., an independent audit might be conducted to report on the entity's conformance with ISO 9001). A third example is the voluntary sustainability report companies are issuing. While sustainability reports may or may not be subject to some form of external assurance, information contained within them is being made publicly available to investors.

3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organization demonstrates a commitment to attract, develop and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Risk Assessment

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.
9. The organization identifies and assesses changes that could significantly impact the system of internal control.

Control Activities

10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
11. The organization selects and develops general control activities over technology to support the achievement of objectives.
12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Information and Communication

13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.
14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
15. The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.

Monitoring Activities

16. The organization selects, develops and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

The principles enable effective operation of the five internal control components and the overall system of internal control. To demonstrate that a principle is present and functioning, the organization must understand the intent of the principle and how it is being applied; work to help personnel understand and apply the principle consistently across the entity; and view weakness in or absence of a principle as requiring management's attention. These are factors management considers when exercising appropriate judgment during the evaluation of internal control. Note that the New Framework does not prescribe specific controls that must be in place. Under a principles-based approach, management identifies controls that impact or influence the principles through their design and execution across the organization.

A principle that is present and functioning operates within a range of acceptability – but does not imply that the organization must achieve the highest level of performance in applying the principle. Management may exercise judgment in assessing the trade-offs between the cost of achieving perfection and the benefits of seeking to operate at various lower levels of performance. There is no one-size-fits-all approach in designing an internal control system.

8. How are points of focus applied?

To enhance the rigor of understanding of each principle, points of focus are provided in the New Framework. Points of focus represent important characteristics associated with the principles and, as such, provide support to the principles to which they pertain. To illustrate, the first principle provided for the Control Environment component is: "The organization demonstrates a commitment to integrity and ethical values." The New Framework provides four points of focus for this principle:

- Sets the "Tone at the Top" – The board of directors and management at all levels of the entity demonstrate through their directives, actions and behaviors the importance of integrity and ethical values to support the functioning of the system of internal control.
- Establishes Standards of Conduct – The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the organization and by outsourced service providers and business partners.
- Evaluates Adherence to Standards of Conduct – Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct.
- Addresses Deviations in a Timely Manner – Deviations from the entity's expected standards of conduct are identified and remedied in a timely and consistent manner.

Many will consider these four points of focus useful when evaluating whether the principle itself is present and functioning. That said, it may be possible to determine that the corresponding principle is present and functioning without all four points of focus. For instance, management may be able to determine that Principle 1 related to integrity and ethical values is present and functioning based on an assessment that only three of the above four underlying points of focus are in place. The organization may set the tone at the top, evaluate adherence to standards of conduct, and address deviations in a timely manner, but it does not formally define the expectations of management and the board of directors in the organization's standards of conduct. In addition, alternative or compensating controls may be in place that provide further support for this conclusion.

As noted in Question 6, it is important to reiterate that the components and principles constitute the criteria that will assist management in assessing whether the components of internal control are present, functioning and operating together within the organization. While points of focus may provide useful guidance to management, the New Framework does not require management to evaluate them separately. As noted earlier, points of focus are mapped directly to the 17 principles. The schedule over the next few pages shows the points of focus underlying each principle, 77 in all and described in a terse manner,[5] as provided by the New Framework.

Note that in the summary below all listed points of focus are numbered sequentially with the exception of three groups of related points of focus germane to Principle 6 that addresses the specification of objectives with sufficient clarity and granularity to provide a context for risk assessment. The content and context of these three groups of points of focus vary depending on the category of objectives being addressed. They are explained further below:

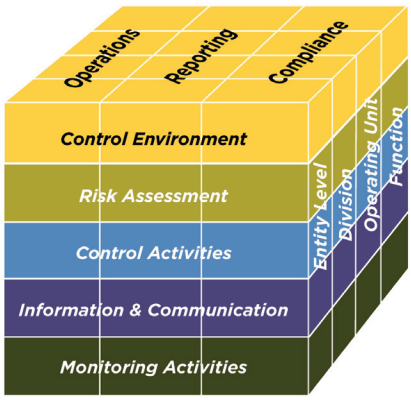
- Point of focus 21 deals with the authority for defining objectives. For example, objectives for external financial reporting are based on the financial reporting assertions provided by "applicable accounting standards" while the objectives for operations and internal reporting are driven by management's discretion (i.e., "reflects

[5] The New Framework includes a more expansive discussion of each of the points of focus.

management's choices"). There are four points of focus in this group – 21a through 21d – related to the five categories of objectives pertinent to Principle 6.

- Point of focus 22 relates to the measurement threshold for applying the reasonable assurance criterion when evaluating the design and operating effectiveness of internal control. For example, the threshold for external financial reporting is the conventional standard of "materiality," whereas the threshold for operations and compliance objectives is management's "tolerances for risk." There are three points of focus in this group – 22a through 22c – related to the five categories of objectives pertinent to Principle 6.
- Point of focus 25 – "reflects entity activities" – applies when external financial reporting, external non-financial reporting and/or internal reporting objectives are addressed when evaluating the effectiveness of internal control.

Note that points of focus 23 and 24 are applied once to operations objectives.



Control Environment			
Principles		**Points of Focus**	
1	**The organization demonstrates a commitment to integrity and ethical values**	1	Sets the tone at the top
		2	Establishes standards of conduct
		3	Evaluates adherence to standards of conduct
		4	Addresses deviations in a timely manner
2	**The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control**	5	Establishes oversight responsibilities
		6	Applies relevant expertise
		7	Operates independently
		8	Provides oversight on Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities
3	**Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives**	9	Considers all structures of the entity
		10	Establishes reporting lines
		11	Defines, assigns, and limits authorities and responsibilities

Control Environment (continued)			
Principles		**Points of Focus**	
4	The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives	12	Establishes policies and practices
		13	Evaluates competence and addresses shortcomings
		14	Attracts, develops and retains individuals
		15	Plans and prepares for succession
5	The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives	16	Enforces accountability through structures, authorities and responsibilities
		17	Establishes performance measures, incentives and rewards
		18	Evaluates performance measures, incentives and rewards for ongoing relevance
		19	Considers excessive pressures
		20	Evaluates performance and rewards or disciplines individuals
Risk Assessment			
Principles		**Points of Focus**	
6	The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives:		
	– Operations Objectives	21a	Reflects management's choices
		22a	Considers tolerances for risk
		23	Includes operations and financial performance goals
		24	Forms a basis for committing of resources
	– External Financial Reporting Objectives	21b	Complies with applicable accounting standards
		22b	Considers materiality
		25	Reflects entity activities
	– External Non-Financial Reporting Objectives	21c	Complies with externally established standards and frameworks
		22c	Considers the required level of precision
		25	Reflects entity activities
	– Internal Reporting Objectives	21a	Reflects management's choices
		22c	Considers the required level of precision
		25	Reflects entity activities
	– Compliance Objectives	21d	Reflects external laws and regulations
		22a	Considers tolerances for risk

Risk Assessment (continued)			
Principles		**Points of Focus**	
7	**The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed**	26	Includes entity, subsidiary, division, operating unit, and functional levels
		27	Analyzes internal and external factors
		28	Involves appropriate levels of management
		29	Estimates significance of risks identified
		30	Determines how to respond to risks
8	**The organization considers the potential for fraud in assessing risks to the achievement of objectives**	31	Considers various types of fraud
		32	Assesses incentives and pressures
		33	Assesses opportunities
		34	Assesses attitudes and rationalizations
9	**The organization identifies and assesses changes that could significantly impact the system of internal control**	35	Assesses changes in the external environment
		36	Assesses changes in the business model
		37	Assesses changes in leadership
Control Activities			
Principles		**Points of Focus**	
10	**The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels**	38	Integrates with risk assessment
		39	Considers entity-specific factors
		40	Determines relevant business processes
		41	Evaluates a mix of control activity types
		42	Considers at what level activities are applied
		43	Addresses segregation of duties
11	**The organization selects and develops general control activities over technology to support the achievement of objectives**	44	Determines dependency between the use of technology in business processes and technology general controls
		45	Establishes relevant technology infrastructure control activities
		46	Establishes relevant security management process control activities
		47	Establishes relevant technology acquisition, development, and maintenance process control activities
12	**The organization deploys control activities through policies that establish what is expected and procedures that put policies into action**	48	Establishes policies and procedures to support deployment of management's directives
		49	Establishes responsibility and accountability for executing policies and procedures
		50	Performs in a timely manner
		51	Takes corrective action
		52	Performs using competent personnel
		53	Reassesses policies and procedures

Information and Communication			
Principles		**Points of Focus**	
13	**The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control**	54	Identifies information requirements
		55	Captures internal and external sources of data
		56	Processes relevant data into information
		57	Maintains quality throughout processing
		58	Considers costs and benefits
14	**The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of other components of internal control**	59	Communicates internal control information
		60	Communicates with the board of directors
		61	Provides separate communication lines
		62	Selects relevant method of communication
15	**The organization communicates with external parties regarding matters affecting the functioning of other components of internal control**	63	Communicates to external parties
		64	Enables inbound communications
		65	Communicates with the board of directors
		66	Provides separate communication lines
		67	Selects relevant method of communication
Monitoring Activities			
Principles		**Points of Focus**	
16	**The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning**	68	Considers a mix of ongoing and separate evaluations
		69	Considers rate of change
		70	Establishes baseline understanding
		71	Uses knowledgeable personnel
		72	Integrates with business processes
		73	Adjusts scope and frequency
		74	Objectively evaluates
17	**The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate**	75	Assesses results
		76	Communicates deficiencies to parties responsible for corrective action and to senior management and the board of directors
		77	Monitors corrective actions

As we stated in an earlier question, the New Framework makes it clear that management has the latitude to exercise judgment in determining the suitability or relevancy of the points of focus it provides. In addition, COSO does not assert the 77 points of focus comprise a complete and comprehensive list. Management may identify and consider other important characteristics germane to a particular principle based on the organization's activities, specific circumstances and regulatory requirements.

9. How are deficiencies in internal control assessed?

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.

The New Framework makes it clear that assessing the severity of a deficiency or combination of deficiencies to determine whether components and relevant principles are present and functioning, and components are operating together, requires judgment. The criteria set forth by the New Framework (i.e., through the components and principles) provide the basis for management to apply judgment when assessing the effectiveness of internal control. In addition, circumstances may arise where management may be required to consider additional criteria established by external parties (e.g., regulators, standard-setting bodies, listing agencies and other relevant third parties). While the New Framework does not prescribe such additional criteria, it recognizes the authority and responsibility of relevant external parties and is flexible enough to accommodate any additional criteria they require, including the manner in which the severity of internal control deficiencies is classified.

Overall, the assessment of the effectiveness of internal control is directed to the five components and their underlying principles. The assessment line of sight addresses whether each of the five components of internal control is present and functioning, the five components of internal control operate together, and the supporting principles are present and functioning, to provide "reasonable assurance" that relevant objectives are met. With respect to how the concept of "major deficiencies" under the 2013 New Framework affects the way companies report internal control deficiencies under Sarbanes-Oxley in the United States, see Question 22.

10. Assume we previously had a clean Section 404 certification but find gaps in the process of mapping our controls documentation to the COSO principles. How will those types of deficiencies be handled? Can we now fail to comply with Sarbanes-Oxley Section 404 requirements if we are weak on a specific COSO principle?

The premise underlying this question is that the organization has completed the mapping exercise and is satisfied that all relevant entity- and process-level controls currently in place have been considered during that exercise. If the mapping of internal controls indicates that the controls in place do not support an assertion that a particular principle is present and functioning, a gap or deficiency exists. In such instances, management will have to evaluate the severity of the deficiency, as explained in Question 9.

11. What are the implications of a deficiency in control design or operation around entity-level type controls?

When evaluating the severity of a deficiency, entity-level controls may present an issue. Ordinarily, a gap in these controls may be deemed a deficiency or significant deficiency rather than a material weakness from a Section 404 compliance standpoint, as their impact on the achievement of the financial reporting objective is not as direct as a

deficiency around a specific process-level control might be. However, over time, identified significant deficiencies will need to be addressed and remediated.

If a deficiency in entity-level controls results in a determination that the corresponding principle is not present and functioning and that determination results in the single component not being present and functioning, then the organization would have a material weakness. This determination is not very likely for entity-level controls because management ordinarily looks for compensating controls in the case of a failure of the primary or key controls.

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

Serious deficiencies in the Control Environment undoubtedly present a formidable problem. In such situations, management should assess these deficiencies in order to determine their magnitude and take appropriate actions to remediate any gaps as soon as possible. Management does not want a situation in which the external auditor has *pervasive* concerns about internal control for which the effect is difficult to determine. For example, a number of significant deficiencies in general IT controls could present significant issues to management and the external auditor. Deficiencies in the Control Environment may necessitate consideration of the other components to ascertain whether deficiencies existing in them may be of greater significance if not remediated on a timely basis. All five components must be evaluated to support management's assertion.

13. What does "present and functioning" mean?

The New Framework states that the phrase "present and functioning" applies to both components and principles. "Present" refers to "the determination that components and relevant principles exist in the design and implementation of the system of internal control to achieve specified objectives." "Functioning" refers to "the determination that components and relevant principles continue to exist in the conduct of the system of internal control to achieve specified objectives." Therefore, ***"present" is about effective design and implementation, whereas "functioning" is about effective operation.*** In determining whether a component of internal control is present and functioning, senior management, with the board of directors' oversight, needs to determine to what extent relevant principles underlying the component are present and functioning.

14. How does management assess whether all components "operate together"?

Evaluating each of the five components of internal control requires consideration of how it is being applied by the entity within the overall system of internal control, and not whether it is functioning on its own. This means that the five components of internal control are an integral part of an effectively functioning system. While management may preliminarily determine that each of the five components is present and functioning, they cannot conclude the organization has effective internal control until a determination is reached that the five components are operating together. To this end, the New Framework states that "operating together" refers to "the determination that all five components collectively reduce, to an acceptable level, the risk of not achieving an objective." "Operating together" recognizes that components are interdependent with a multitude of interrelationships and linkages, particularly in terms of how principles interact within and across components. From a practical standpoint, the New Framework states that ***management can demonstrate that components operate together when they are present and functioning and internal control deficiencies aggregated across components do not result in the determination that one or more major deficiencies exist.***

To illustrate the inherent interdependencies and linkages among components, the development and deployment of policies and procedures as part of Control Activities contributes to the mitigation of risks identified and analyzed within Risk Assessment. For another illustration, the communication of internal control deficiencies to those responsible for taking corrective action as part of Monitoring Activities reflects a full understanding of the

entity's structures, reporting lines, authorities and responsibilities as set forth in the Control Environment and as communicated within Information and Communication. The New Framework includes other examples.

15. Are external parties who do not process transactions a part of the system of internal control?

External parties, including external auditors and regulators, who do not have responsibility for processing transactions are not part of the system of internal control, and cannot be considered a source of detection and assessment of internal control deficiencies when a company assesses the effectiveness of its internal control structure. Responsibility for identifying and assessing internal control deficiencies rests with the organization's personnel, in the normal course of performing their ongoing functions. Note that outsourced or third-party service providers are covered in the following question.

16. Are outsourced service providers a part of the system of internal control?

COSO references the concept of outsourced business processes in several places in the New 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 in processing its information, is subject to the same internal control expectations. When outsourced service providers perform controls on behalf of the entity, the framework provides the following guidance:

- 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 supporting the organization's ability to rely on such information include internal control over outsourced service providers such as vendor due diligence, inclusion of right-to-audit clauses in service agreements, exercise of right-to-audit clauses, and obtaining an independent assessment over the service provider's controls that is sufficiently focused on relevant control objectives.
- The blurred lines of responsibility between the entity's internal control system and that of outsourced service providers create a need for more rigorous controls over communication between the parties.
- Monitoring applies to outsourced service providers just as it does internal processes. To that end, the framework provides specific guidance to consider.

The above considerations represent factors for management to take into account when evaluating the system of internal control.

17. When are we required to apply the New Framework?

This question is relevant for organizations that already use the 1992 framework. This is particularly the case for companies that will apply the New Framework to their Sarbanes-Oxley compliance efforts.

The COSO Board has stated that users should transition to the 2013 New Framework in their applications and related documentation as soon as it is feasible given their particular circumstances. COSO will continue to make available the original 1992 framework through December 15, 2014, after which time it will consider the framework as having been superseded. The COSO Board believes the key concepts and principles embedded in the original version of the framework are fundamentally sound and broadly accepted in the marketplace and, accordingly, considers it appropriate for companies to continue their use of the original version during the

transition period (May 14, 2013 to December 15, 2014). This means calendar-year companies may apply the 1992 version to calendar year 2013, and must transition to the New Framework for purposes of applying it by no later than calendar year 2014.

Non-calendar-year reporting companies may also adopt as early as is feasible, but would be expected to have completed their transition by their assessment of the effectiveness of ICFR for their first year ended after December 15, 2014. For example, assume a June 30 year-end reporting company must comply with Sarbanes-Oxley Section 404. Because December is midyear for this company, the transition deadline would apply to its fiscal year ended June 30, 2015. Stated another way, since the 1992 framework isn't superseded until December 15, 2014, it is still sound as of June 30, 2014. This guidance implies that the 2013 New Framework should be in place at the time a company begins its assessment of ICFR for the corresponding fiscal year.

Questions also arise as to whether quarterly reports issued by non-calendar-year reporting companies after December 15, 2014 require adoption of the 2013 New Framework. For example, assume a June 30 year-end reporting company intends to transition to the 2013 New Framework for purposes of its evaluation of ICFR as of June 30, 2015. Would the quarterly reports (e.g., Form 10-Q) filed for interim quarters ended December 31, 2014 and March 31, 2015 leading up to the June 30, 2015 fiscal year-end require a transition to the New Framework because they were issued after December 15, 2014? Typically, the Form 10-Q quarterly report refers back to the evaluation in the previously filed annual report on Form 10-K with no reference to the "suitable framework" used to evaluate ICFR. The primary focus of the quarterly 10-Q is to identify whether a material change in ICFR has occurred. Therefore, from a financial reporting perspective, we have advised our non-calendar-year reporting clients that the transition to the New Framework would be expected to apply to their 2015 10-K.

COSO is not a regulator. Therefore, it cannot mandate actions by issuers. However, its declaration that the 1992 framework will be superseded by the 2013 New Framework as of December 15, 2014 will make it difficult for any issuer to take the position that the superseded framework qualifies under the SEC's criteria as a "suitable framework" for purposes of complying with Section 404 of Sarbanes-Oxley.

18. What is the SEC's position on transitioning to the New Framework?

As of the date this publication was released, the SEC had not issued an official position on the transition question insofar as compliance with Section 404 is concerned. In a speech, a member of the SEC staff indicated that the staff plans to monitor the transition for issuers using the 1992 framework. Specifically, the SEC staff's remarks were as follows:[6]

> I understand that COSO intends to supersede their 1992 Framework as of December 15, 2014, and we expect there will be questions about whether the SEC will provide management with any transition or implementation guidance to change from the existing framework to the new framework. COSO has publicly stated its belief that "users should transition their applications and related documentation to the updated Framework as soon as is feasible under their particular circumstances" and that "the key concepts and principles embedded in the original framework are fundamentally sound and broadly accepted in the marketplace, and accordingly, continued use of the 1992 framework during the transition period (May 14, 2013 to December 15, 2014) is acceptable." COSO further explained "the COSO Board's goal in updating the original Framework has been to reflect changes in the business and operating environments, to formalize more explicitly the principles embedded in the original framework that facilitate development of effective internal control and assessment of its effectiveness, and to increase the ease of use when applied to an entity objective."
>
> [The] SEC staff plans to monitor the transition for issuers using the 1992 framework to evaluate whether and if any staff or Commission actions become necessary or appropriate at some point in the

[6] Remarks made at the 32nd Annual SEC and Financial Reporting Institute Conference by Paul Beswick, chief accountant of the Office of the Chief Accountant of the SEC, May 30, 2013; documentation available on the SEC website at http://www.sec.gov/News/Speech/Detail/Speech/1365171575494.

future. However, at this time, I'll simply refer users of the COSO framework to the statements COSO has made about their new framework and their thoughts about transition.

The SEC has a long-standing practice of not issuing guidance when the private sector's procedures appear to be working. This appears to be the case here, as COSO has done the heavy lifting and the SEC staff has simply said they will watch issuers closely – and they seem to mean what they say. We believe that the SEC staff is supportive of COSO's suggested approach for transitioning from the 1992 framework to the 2013 New Framework. We also believe the SEC staff's statement implies the staff expects issuers to transition from the superseded 1992 framework within the time frame provided by COSO.

19. What if we continue to apply the original framework beyond COSO's transition period?

For companies complying with Sarbanes-Oxley, we do not believe this would be a wise choice. During the transition period, the COSO Board believes that application of its *Internal Control – Integrated Framework* that involves external financial reporting should clearly disclose whether the original or 2013 version was utilized. As noted above, the SEC staff has sent a clear signal that they intend to monitor the transition from the 1992 framework. Accordingly, we believe there is a presumption that only the 2013 New Framework will be in use after the transition period expires. Companies are likely to receive pushback from their external auditors – and perhaps from the SEC staff as well – if they continue to use the superseded 1992 framework.[7]

If a calendar-year reporting company elected to use the 1992 framework for purposes of the 2014 assessment, the SEC staff will likely issue a comment letter. Given that COSO will have superseded the 1992 framework as of that time, it would be difficult to convince the SEC staff or anyone else that the 1992 framework represents a "suitable framework" for purposes of complying with Sarbanes-Oxley Section 404. The external auditors will likely not support a company's decision to use the 1992 framework once it is superseded and could even conclude that a deficiency exists for purposes of communicating to the audit committee. Therefore, we would not recommend testing the audit firms with a view of this nature.

20. Must we begin applying the 2013 New Framework in the first quarter of 2014 for purposes of complying with Section 302 of Sarbanes-Oxley?

Section 302 of Sarbanes-Oxley requires an executive certification each quarter. This certification refers to ICFR in several ways. For example, the certifying officers must indicate the following:

- They are responsible for establishing and maintaining "internal control over financial reporting" for the issuer;
- They have designed ICFR, or caused such ICFR to be designed under their supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;
- They certify that they have disclosed any change in the issuer's ICFR that occurred during the issuer's most recent fiscal quarter that has materially affected, or is reasonably likely to materially affect, the issuer's ICFR; and
- Based on their most recent evaluation of ICFR, they have disclosed significant deficiencies, material weaknesses and fraud to the auditors and to the audit committee.

[7] SEC staff may issue implementation guidance on this point. However, in the absence of such guidance, the staff could raise concerns if issuers use the 1992 version as a "suitable framework" after December 15, 2014.

The question arises for a calendar-year reporting company as to whether the above references to ICFR in the quarterly executive certification require the use of the 2013 New Framework beginning in the first quarter of 2014.

This is a legal question and companies are advised to consult with their legal counsel. In our view, it has been a long-standing practice that the Section 302 assessment of ICFR be based on the most recent Section 404 assessment. The SEC has made it clear that Section 302 does not 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, as noted above, would be the consideration of the effect of changes in ICFR to ascertain their significance for disclosure purposes.

We believe 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. Furthermore, the Section 404 assessment is an "as of" assessment as of the end of the year and the tests to validate design and operating effectiveness are substantially the same under the 1992 or 2013 versions of the COSO internal control framework. That being stated, we believe it is important that as the company transitions to the 2013 New Framework the activities undertaken to support the Section 302 process are aligned with the transition.

21. What are the implications for Sarbanes-Oxley compliance?

As discussed earlier, the company must clearly disclose in its internal control report whether the original or 2013 version was utilized during the transition period. In addition, the existing internal control documentation must be converted to the principles-based approach of the New Framework. For companies that have experienced the rigor of several years of compliance under Section 404 of Sarbanes-Oxley, we do not believe this will be a significant undertaking. To illustrate, the seven factors for the Control Environment under the original 1992 version can be organized easily under the five principles provided in the 2013 New Framework.

Note that the New Framework and related illustrative documents consist of an executive summary, the actual New Framework itself, several appendices, an applications guide providing illustrative tools, and a separate compendium of approaches and examples for application of the New Framework to ICFR. The latter compendium may be useful to companies complying with Sarbanes-Oxley.

Following is commentary regarding certain principles in conjunction with the evaluation of ICFR in accordance with Section 404 of Sarbanes-Oxley:

- ***Principle 6: The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to the objectives*** – The points of focus around the objective for external financial reporting relate to established financial reporting assertions and materiality considerations, and reflect the entity's activities. These are the same objectives that organizations have been using for the Section 404 risk assessment since its inception.

- ***Principle 7: The organization identifies risks to the achievement of objectives across the entity and analyzes risks as a basis for determining how the risks should be managed*** – A good place to start is to map existing documentation supporting Risk Assessment to the related points of focus. Each organization may approach this differently, but much of this material may already exist in various forms. For example, a memorandum outlining the process may be warranted, linking the various activities to how the entity accomplishes the selected points of focus.

- ***Principle 8: The organization considers the potential for fraud in assessing risks to the achievement of objectives*** – Many companies integrate their evaluation of the effectiveness of controls mitigating fraud risk with the evaluation of other controls embedded within the organization's processes. The underlying

premise is that control activities are an integral part of making business processes work. Embedded within the processes, they provide assurance that the processes are preventing and detecting errors and fraud on a timely basis, and as close as possible to the source, providing assurance that relevant financial reporting assertions are met. Control activities are in place within the process to reduce "financial reporting assertion risks" to an acceptable level, *including the risk of fraud*. The financial reporting assertions and the risks ("what can go wrong") associated with achieving those assertions provide a context for evaluating the design effectiveness of control activities at the process level. Fraud risk is often worked into the identification of the risks; therefore, many companies embed their assessment of fraud risk into their overall assessment of financial reporting risk. Protiviti and, to the best of our knowledge, most accounting firms have supported this integrated approach, provided that fraud scenarios common to the industry are appropriately considered.

The question arises as to whether the articulation of Principle 8 will require separate documentation. This is a matter warranting discussion in the early stages of the transition process to ensure that the appropriate steps are undertaken. Some companies conduct an assessment of the anti-fraud program and controls. For those issuers currently conducting a separate assessment focused on the anti-fraud program, the matter of documentation will be a relatively simple matter. However, for issuers that have integrated anti-fraud controls into their process documentation, the documentation may not be quite as clear, and it may make it more difficult to identify those controls. In some instances, it may make sense to determine through dialogue with the external auditors their expectations and requirements, inventory the elements of the anti-fraud program currently in place and under development, and document an overall summary of the significant fraud risks and how they are addressed through the anti-fraud program. In other cases, the transition to the New Framework may present a good opportunity to reconsider whether the issuer's anti-fraud program is robust enough. For example, are all fraud risks considered?

- ***Principle 10: The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels –*** While this principle doesn't present anything new, it does emphasize the fundamental purpose of ICFR, which is to reduce the risk of material errors or omissions in the financial statements to an acceptable level. Issuers that have focused their Section 404 documentation on the achievement of financial reporting objectives may need to redirect their focus on the reduction of risk to the achievement of the objectives to an acceptable level. This may mean documenting what an "acceptable level of risk" is using the context of materiality.

- ***Principle 11: The organization selects and develops general control activities over technology to support the achievement of objectives –*** The evaluation of general technology controls in conjunction with evaluating the effectiveness of ICFR is not new. What is new is the emphasis Principle 11 gives to this area, which raises the question regarding sufficiency of scope and documentation. This is another matter warranting discussion in the early stages of the transition process to ensure that the documentation is completed appropriately during the controls mapping process. To this point, it may make sense to determine through dialogue with the external auditors their expectations and requirements and document an overall summary of the work done to address the general technology controls.

- ***Principle 13: The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control –*** This is an area that has always required careful consideration in an assessment of ICFR. Many control activities rely on the reliability and timeliness of reports over time. To evaluate the controls without considering the reliability of the reports used in executing the controls is an incomplete assessment. This point has been stressed by the Public Company Accounting Oversight Board (PCAOB) in their inspection reports. Typically, this matter is considered an integral part of testing the operating effectiveness of ICFR. Accordingly, it warrants discussion in the early stages of the transition process to ensure that the documentation is completed appropriately during the controls mapping process. The points of focus provided by the 2013 New Framework – identifies information requirements, captures internal and external sources of data, processes relevant data into information, maintains quality throughout processing, and considers costs and benefits – may be useful in thinking through how to document this principle.

- ***Principle 14: The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control –*** The New Framework states that communication is the continuous, iterative process of providing, sharing, and obtaining information throughout the organization, flowing up, down, and across the entity. Internal information enables personnel to receive a clear message from senior management regarding their control responsibilities. The points of focus for this principle – communicates internal control information, communicates with the board of directors, provides separate communication lines, and selects relevant method of communication – may be useful in thinking through how to document this principle.

- ***Principle 15: The organization communicates with external parties regarding matters affecting the functioning of other components of internal control –*** The New Framework states that the focus on external communications is twofold. First, it enables inbound communication of relevant external information necessary to assess risks, conduct control activities, and monitor risks and controls. Second, it provides information relating to ICFR to external parties in response to requirements and expectations. The points of focus for this principle – communicates to external parties, enables inbound communications, communicates with the board of directors, provides separate communication lines, and selects relevant method of communication – may be useful in thinking through how to document this principle.

- ***Principle 17: The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate –*** Again, nothing new here. The principle emphasizes the importance of decisive and timely action when dealing with internal control deficiencies.

A final point is the aggregation and consideration of internal control deficiencies. This is an area where companies will want to be on the same page as their external auditors. Factors to consider when evaluating deficiencies are their nature and source, the known magnitude of a misstatement they have caused to the issuer's financial statements, the likelihood and potential magnitude of a misstatement that deficiencies could cause to the issuer's financial statements, and the aggregate effect of deficiencies affecting similar areas that could indicate a more serious deficiency.

22. How will the concept of "major deficiencies" under the 2013 New Framework affect the way companies report internal control deficiencies under Sarbanes-Oxley?

We don't see any additional effect. The nomenclature adopted by COSO in the 2013 New Framework was intended to be universal across country borders and regulatory regimes. The New Framework states:

> Reporting on internal control deficiencies depends on the criteria established by regulators, standard-setting bodies, and management and boards of directors, as appropriate. Results of ongoing and separate evaluations are assessed against those criteria to determine whom to report to and what is reported. Alternatively, any criteria established by the board of directors or management typically [are] based on the entity's facts and circumstances and on established laws, rules, regulations, and standards.

The criteria in the United States 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. Because the components being present and functioning are a primary focal point in reviewing the effectiveness of internal control, including ICFR, a major deficiency under COSO would most likely translate to a material weakness for Section 404 compliance purposes.

23. Does the 2013 New Framework affect the way companies evaluate their controls over technology?

The 2013 New Framework is updated for the more sophisticated, decentralized and mobile technology environments existing today that involve multiple, real-time activities cutting across myriad systems, organizations and processes. Since the 1992 framework was issued, technology has evolved as have the techniques and methodologies for evaluating the design effectiveness and operating effectiveness of controls over technology.

The COSO *Internal Control – Integrated Framework* provides an overall framework for addressing the effectiveness of internal control in providing reasonable assurance that operational, reporting and compliance objectives are achieved. It is not prescriptive. Because of the granularity needed in addressing technology controls, some use other tools to facilitate their evaluation of technology controls. For example, the Information Systems Audit and Control Association's (ISACA) Control Objectives for Information and Related Technology (COBIT) framework provides overall guidance on the achievement of the broader spectrum of internal control surrounding certain aspects of the technology control environment. In this context, while the COSO framework should be considered as an overall evaluation framework for internal control, COBIT provides useful guidance and background material in the consideration of specific controls over technology.

In the COSO New Framework, there is a separate principle relating to general controls over technology (Principle 11). In addition, the New Framework acknowledges that when technology is embedded into the entity's business processes (such as robotic automation in a manufacturing plant), control activities are needed to mitigate the risk that the technology itself will not operate properly to support the achievement of the organization's objectives. In addition, the New Framework states many control activities in an organization are partially or wholly automated using technology. These procedures are known as automated control activities or automated controls in the New Framework. There isn't anything new with these points, as they have been considered in practice over the years when evaluating the effectiveness of internal control.

Experience has demonstrated that most business processes have a mix of manual and automated controls, depending on the availability of technology in the entity. The New Framework states that automated controls tend to be more reliable, subject to whether technology general controls are implemented and operating, since they are less susceptible to human judgment and error, and are typically more efficient. Again, this point of view reflects a long-standing practice.

Protiviti's *Guide to the Sarbanes-Oxley Act: IT Risks and Controls (Second Edition)*, available at **www.protiviti.com**, provides guidance to Section 404 compliance project teams on the consideration of IT risks and controls at both the entity and activity levels within an organization. Questions and answers in the guide focus on the interaction between the IT organization and the entity's application and data process owners, and explain the implications of general IT controls and how they are considered at the process level. This guide also explores how application control assessments are integrated with the assessment of business process controls, and addresses documentation, testing and remediation matters.

24. How do we disclose in our annual internal control report which framework we used during the transition period?

In the internal control report, management must disclose the framework used as criteria for evaluating the effectiveness of ICFR. In making this disclosure when using the COSO framework as a "suitable framework" as directed by the SEC, companies typically use language along the lines of "criteria established in the *Internal Control – Integrated Framework* issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO)." While practice will evolve, when companies issue an internal control report during the transition period, they may place a parenthetical reference – either "(1992)" or "(2013)" – after "*Internal Control – Integrated Framework*." Whether such disclosure will be needed or customary after the transition period expires remains to be seen.

25. What do we need to do now?

Companies that currently use the original 1992 framework must determine their transition plan to evolve from it to the 2013 New Framework. For example, for calendar-year companies, does the company apply the 2013 New Framework before December 15, 2014 or continue to use the 1992 version? In addition, once the transition plan is defined, it should be communicated to senior management and the audit committee.

26. What tasks are necessary in transitioning to the 2013 New Framework?

In getting started, those responsible for the transition process should familiarize themselves with the framework and consider attending available training. Depending on the nature and timing of the transition plan, companies may want to deploy a centralized, project management office (PMO)-like discipline to ensure a top-down, cost-effective approach to converting the underlying documentation to support a determination that the underlying principles outlined in the New Framework are present and functioning. This approach would entail designating roles, responsibilities and authorities for converting the documentation.

The principles should be mapped to the organization's existing controls documentation so that management can evaluate the body of evidence that supports a preliminary conclusion that the principles are present and functioning. Ideally, the existing controls documentation will provide most, if not all, of the input to this mapping exercise, particularly if the company has previously documented its controls in a rigorous fashion using the 1992 version of the framework. Presumably, companies have followed a top-down, risk-based approach in identifying their key controls in prior years, and the mapping process should mirror that approach. In completing the mapping exercise, provisions should be made for mapping a single control to multiple principles if it is relevant to those principles.

If there are gaps for certain principles, the company will need to ascertain whether additional controls exist or controls require strengthening to support a conclusion that those principles are present and functioning. Once all of the gaps are addressed, management presumably is in a position to conclude the components are present and functioning. Then, management can evaluate whether the five components of internal control operate together.

In finalizing the mapping approach, the expectations of the external auditor should be considered to ensure the audit requirements are addressed without resorting to costly rework following the completion of the conversion process. In addition, the internal audit function should begin focusing on its transition to the New Framework for purposes of planning, conducting and reporting on risk-based audits. A communications plan also would be appropriate (see Questions 33 and 34).

Although the desired end result of issuing the New Framework is not intended to create another "checklist," it's possible a checklist will be employed somewhere, by someone – including possibly by the external auditors. When the PMO (or equivalent group) maps the principles supporting the five components to the organization's controls, management may desire to use the points of focus provided by the New Framework. Assuming management intends to use points of focus when evaluating whether the principles to which they apply are present and functioning, given the New Framework's commentary regarding points of focus, management should assess whether they are suitable, relevant and complete based on the company's specific circumstances. The PMO (or equivalent group) can ensure that this assessment occurs.

27. What is the level of effort required to map the principles to the existing controls?

The level of effort of transitioning the existing controls documentation to the principles-based New Framework will depend on a number of factors, such as:

- The size and complexity of the company (e.g., for how many units must the issuer document the entity-level controls)
- The extent to which the issuer has kept the controls documentation current for changes in the business over time
- Whether the issuer used the principles-based guidance provided by COSO to small companies[8]
- The expectations of the external auditor regarding the nature and extent of the documentation they require to audit the effectiveness of ICFR using the New Framework

[8] See *Internal Control over Financial Reporting — Guidance for Smaller Public Companies*, 2006, available at www.coso.org.

The reality at this time is that few companies have done the mapping. Therefore, there is no simple answer to the level-of-effort question. For this reason, it is important to begin the planning process soon.

28. Who should complete the mapping of controls to the 17 principles?

Whoever is charged with the responsibility for executing management's internal control evaluation for Sarbanes-Oxley compliance and other purposes should also be responsible for completing the mapping exercise. In some organizations, this is a separate internal controls group. In others, it is internal audit working in conjunction with management. In still others, it may be the risk owners. Once the mapping process is complete, internal audit could review this work and provide assurance regarding its completeness and sufficiency provided another group executed the process.

29. What are the components of a model project plan for 2013 New Framework implementation?

While plans vary from company to company, our work assisting companies with formulating customized plans has raised a number of points to consider. Following is a high-level outline of some of the major points, which presumes the company's focus is on evaluating ICFR in accordance with Section 404 of Sarbanes-Oxley in the United States or similar legislation in other countries:

- Set the foundation for getting everyone on board
  - Conduct internal discussions
  - Present overview of framework to certifying officers and audit committee
  - Summarize the key changes to existing evaluation approaches
  - 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
  - Identify the necessary resources
- Conduct an initial discussion with the external audit firm to obtain their views on the approach and any issues they see with respect to the company. For example:
  - Determine their expectations on changes in documentation
  - Understand the key changes they see related to the company's previous approach
  - Identify areas that could be more difficult and require attention to address specific challenges
- Create the 17 principles documentation inventory using an appropriate spreadsheet application, an automated software conversion module or some other tool. Create a document that:
  - Lays out the 17 principles and, under each principle, summarizes at a high level "what the company has that demonstrates this principle is present and functioning"
  - Formulates an initial conclusion with respect to controls supporting each principle using appropriate criteria. For example: we have it nailed (we're done); we are in pretty good shape with some refinements needed; we have some controls that are relevant but have work to do to complete our documentation; or we must start from scratch (we have very little documentation)
  - Uses this perspective to plan the focus of the mapping exercise

- Map the organization's controls to the 17 principles and come to a preliminary conclusion regarding (1) whether the design of the documented controls is effective (which supports a determination that the principle is "present") and (2) if the controls are determined to be operating effectively, whether they would allow management to assert that the principle is "present and functioning." Based on the work above:
  - Determine the controls that must be reconfigured, changed, added or deleted for 2014, if any, to support a positive assertion in the company's internal control report
  - 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, identify areas for further emphasis and revision, determine the remaining action plan, and so forth
- Execute remaining steps in the action plan and monitor progress to completion

While not intended to be all-inclusive or a one-size-fits-all solution, the above outline provides a practical starting point for most organizations.

30. When we map our controls to the principles underlying the five components, where do entity-level controls fit in relative to process-level controls? Are the controls being mapped to the points of focus primarily entity-level controls, or are they also inclusive of process-level controls depending on the sufficiency of the entity-level controls within the organization?

A top-down, risk-based approach should drive the mapping exercise. The controls that get mapped to the 17 principles supporting the five components may or may not be considered entity-level controls. It will vary in each organization.

Most traditional controls supporting reliable financial reporting fall in the Control Activities component (which maps to three of the 17 principles), some map to the Monitoring principles (which cover two other principles), and some map to the Information and Communication principles embedded in the business cycles (while part of Information and Communication also covers entity-level type controls). For example, Principle 13 of the Information and Communication component addresses relevant quality information to support the functioning of other components of internal control, particularly Control Activities and Monitoring.

The nature of the Control Environment component lends itself primarily to map directly to entity-level controls. In the Risk Assessment component, the principle addressing objective-setting for external financial reporting focuses on established financial reporting assertions and materiality considerations, and reflects entity-level activities. As such, this principle most likely maps to the organization's risk assessment and scoping exercise around evaluating the effectiveness of ICFR. The other Risk Assessment principles could be either embedded in the Control Activities documentation or evaluated separately from an entity-level perspective. For example, many organizations have integrated their fraud risk assessment into their Section 404 documentation rather than having a separate risk assessment for fraud on a stand-alone basis. The "right answer" will depend on each organization's facts and circumstances.

The above discussion is very high-level and is provided without context to a specific organization's circumstances. There is no one-size-fits-all solution for mapping controls to the 17 principles, as the structure, risks and operating style of each organization will have an impact on the appropriate mapping process.

31. Does the 2013 New Framework alter the approach to complying with Section 404 to also consider Operations and other Compliance objectives in conjunction with our Section 404 compliance activities?

No. Most companies use a top-down, risk-based approach in evaluating the effectiveness of their ICFR, as recommended by the SEC's 2007 Interpretive Guidance[9] and as emphasized by Auditing Standard No. 5. The 2013 New Framework does not alter that approach. The companion *Internal Control over External Financial Reporting Compendium* generally supports a top-down, risk-based approach.

The Section 404 assessment is focused solely on the external financial reporting objective. As such, the Operations objective does 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. 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 1992 framework. The New Framework expanded explanations for the non-ICEFR objective categories in order to broaden its use in conjunction with 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.

32. What are the implications of the 2013 New Framework, if any, for a company's internal audit and other risk management functions beyond compliance with Sarbanes-Oxley and other similar regulations relating to financial reporting controls?

The COSO framework was developed more than a decade before the Sarbanes-Oxley Act and other similar legislation was enacted in the United States and other countries. Like its 1992 counterpart, the 2013 New Framework is also intended to have applicability well beyond a company's financial reporting controls. Many internal audit charters reference the COSO *Internal Control – Integrated Framework* as the framework that they apply in support of their internal audit activities around planning, execution and reporting. As such, the same transition deadlines apply to these functions as well.

Many organizations may find it useful to begin the transition to the New Framework through the annual or ongoing risk assessment process conducted by the company's internal audit function, as well as by risk management and compliance management functions. For calendar-year-end reporting companies, this assessment activity may have been initiated in 2013 or now can be immediately incorporated into ongoing risk assessment efforts. These activities may provide a good starting point for organizational transition plans, and also allow the company to use an existing process as another touchpoint to communicate and educate key stakeholders about the transition to the New Framework. For some companies, this may be too early due to resource constraints. In such instances, it is acceptable to apply the 2013 New Framework in the fourth quarter of 2014 for purposes of conducting risk assessments that will drive 2015 internal audits and risk and compliance management priorities. COSO is not mandated for use by The IIA; however, as a sponsoring organization of COSO, The IIA would likely endorse any chief audit executive's decision to adopt the New Framework as a tool for planning, executing and reporting internal audit work.

33. To whom do we communicate – and what do we tell them?

For companies that currently use the original framework in their Sarbanes-Oxley compliance, communications are likely needed to the certifying officers and the audit committee. These executives and directors should be informed of the release of the New Framework, what's new, what's unchanged, the company's recommended transition plan, the company's disclosure obligations during the transition period, and any issues envisioned for the transitioning process.

---

[9] See *Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934*, available at http://www.sec.gov/rules/interp/2007/33-8810.pdf.

34. What do we communicate to the audit committee?

Audit committees have the following questions:

- What are the major changes COSO has made to the *Internal Control – Integrated Framework*?
- How does the 2013 New Framework impact management's approach to complying with Sarbanes-Oxley Section 404?
- How is management complying with Sarbanes-Oxley Section 404 this year (i.e., which version of the COSO Framework is the company using – 1992 or 2013)?
- What are the disclosure ramifications if management intends to use the 1992 framework this year?
- What is management's transition plan to the 2013 New Framework?

This publication will help prep management for the above conversation.

35. What if we adopt the 2013 New Framework this year for ICFR but not for other operational, compliance and reporting areas: Can we still disclose we have adopted the New Framework in this year's internal control report?

Yes. There is nothing in the New Framework specifically addressing this question; however, as embodied in the cube, the New Framework is designed to be flexible in application to different objectives. Furthermore, management's assertion in the internal control report required by Section 404 of Sarbanes-Oxley is directed solely to the effectiveness of ICFR. Therefore, management may refer to the New Framework in the internal control report as long as the issuer has fully adopted it in evaluating the effectiveness of ICFR. In making the disclosure, the internal control report will need to include the 2013 parenthetical reference (see Question 24).

36. Will there be a "street reaction" to companies that do not "early apply"?

For companies that currently use the 1992 version of the framework in their Sarbanes-Oxley compliance, we do not believe there will be any market repercussions if they decide to apply the 1992 version of the framework during the transition period. COSO has laid out an orderly process for transitioning to the New Framework, and the COSO Board asserted that the 1992 version is fundamentally sound and broadly accepted in the marketplace.

37. Does the New Framework comment on the limitations of internal control?

Yes. While internal control provides important benefits, the New Framework makes clear that limitations do exist. Limitations may result from the quality and suitability of objectives established as a precondition to internal control; the potential for flawed human judgment in decision-making; management's consideration of the relative costs and benefits in responding to risk and establishing controls; the potential for breakdowns that can occur because of human failures (such as simple errors or mistakes); the possibility that controls can be circumvented by collusion of two or more people; and the ability of management to override internal control functions and decisions. These limitations preclude the board and management from ever having absolute assurance of the achievement of the entity's objectives. Therefore, controls only provide reasonable – but not absolute – assurance.

38. How do we use the illustrative tools for assessing effectiveness of a system of internal control?

The illustrative tools publication is intended to assist management when using the New Framework to assess whether each of the five components and relevant principles is present and functioning, and the five components are operating together in an integrated manner. The purpose of the illustrative tools is limited to illustrating one possible assessment process based on the requirements for effective internal control, as set forth in the New Framework. Not to be used in lieu of the New Framework, it is organized into two sections. The templates section provides templates that can support and document an assessment of the effectiveness of a system of

internal control. The scenarios section illustrates several practical examples of how the templates can be used to support an assessment of effectiveness of a system of internal control. Together, the templates and scenarios focus on evaluating components and relevant principles and present only a summary of assessment results, and do not focus on evaluating the underlying controls (e.g., transaction-level control activities) that affect the relevant principles. COSO makes it clear that the templates are illustrative and are not an integral part of the New Framework, and may not address all matters that need to be considered when assessing a system of internal control. Furthermore, they are not intended to represent a "preferred method" of conducting and documenting an assessment.

39. Why did COSO issue the *Internal Control over External Financial Reporting: A Compendium of Approaches and Examples*?

According to COSO, the intent of the Compendium is to help users apply the New Framework to internal control over external financial reporting (ICEFR). Therefore, the Compendium is a companion publication to the New Framework that provides approaches and examples to illustrate how entities may apply the principles set out in the New Framework to a system of ICEFR. It provides practical approaches and examples that illustrate how the components and principles set forth in the New Framework can be applied in designing, implementing and conducting internal controls over the preparation of external financial statements. The approaches and examples relate to each of the five components and 17 principles set forth in the New Framework and illustrate how various characteristics of principles may be present and functioning within a system of ICEFR objectives; however, they do not attempt to illustrate all aspects of the components and relevant principles necessary for effective ICEFR. The approaches describe how organizations may apply the related principles within their system of ICEFR to give users a summary-level description of activities that management may consider as they apply the New Framework in an ICEFR context. The examples provide specific illustrations to users on the application of each principle, based on situations drawn from practical experiences and illustrating one or more points of focus germane to the principle.

40. Are we required to use COSO's External Financial Reporting Compendium?

While the Compendium is a supplemental document that can be used in concert with the New Framework when considering ICEFR, it neither replaces nor modifies the New Framework. In the context of Sarbanes-Oxley compliance in the United States, the extent to which the Compendium is likely to be used depends on the experience of the issuer with the compliance process. For newly public companies or companies that are contemplating an initial public offering, the Compendium can definitely help them apply the New Framework to ICEFR. For established companies that have complied with Section 404 for several years, including the auditor attestation provisions, they are likely to use the Compendium on a selective basis to understand how they can convert their existing documentation under the 1992 framework to the principles-based structure of the New Framework or in situations involving changes in conditions and processes.

COSO never intended for the Compendium to be used in lieu of the New Framework. The New Framework is the authoritative standard. In addition, COSO pointed out caveats regarding overreliance on the Compendium. COSO did not attempt to illustrate all aspects of the components and relevant principles necessary for effective ICEFR in the Compendium. While the approaches and examples in the Compendium are intended to illustrate how principles may be present and functioning, they are not sufficient to enable an organization to determine that each of the five components and relevant principles is present and functioning. While the examples provide specific illustrations to users on the application of each principle, based on situations drawn from practical experiences and illustrating one or more points of focus germane to the principle, they are not designed to provide a comprehensive example of how the principle may be fully applied in practice. Thus, the approaches and examples are samples of activities for management to consider, rather than a complete or authoritative list. In summary, readers should refer to the New Framework for a comprehensive discussion of how entities design, implement, and conduct a system of internal control, and for the requirements of effective internal control.

41. How does the New Framework apply to smaller companies?

Appendix C, on pages 198 through 202 of the New Framework, discusses the characteristics of smaller entities and meeting the challenges they face in attaining cost-effective internal control.

42. When using the COSO framework for a nonprofit or nonpublic entity, do the 17 principles need to be present and functioning for these "smaller" nonpublic entities?

The COSO framework is written to be used by 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 that is relevant to nonprofit or privately held 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 difficult to attract independent directors with the desired skills and experience to provide appropriate oversight (Principle 2). 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, or concerns about potential personal liability. That limitation does not eliminate the importance of Principle 2 to internal control.

43. Does the New Framework supersede COSO's guidance on Monitoring?

No. COSO issued its *Guidance on Monitoring Internal Control Systems* (COSO Monitoring Guidance) in 2006. That guidance elaborated on the Monitoring component of internal control, as further discussed in the 1992 framework. The 2013 New Framework does not supersede the COSO Monitoring Guidance, as this guidance helps organizations recognize and maximize the use of monitoring when it is effective and enhance monitoring in areas where improvement may be warranted. The guidance also provides practical illustrations on how monitoring can be incorporated into an organization's internal control processes addressing all three objectives incorporated in the COSO *Internal Control – Integrated Framework*. Therefore, it remains a valuable reference. The COSO Monitoring Guidance does not change any of the fundamental elements of the COSO *Internal Control – Integrated Framework*.

44. How is the 2013 New Framework, and specifically the 17 principles, applied to evaluate internal control over compliance?

The Framework is very adaptable to compliance. The following discussion addresses the 17 principles using the five components of the New Framework.

- The *Control Environment* as supported by Principles 1 through 5, sets the tone for compliance and every other area of internal control. The five principles deal with: (1) commitment to integrity and ethical values; (2) independent board oversight; (3) establishment of appropriate structures, reporting lines, and appropriate authorities and responsibilities; (4) commitment to attracting, developing and retaining competent people; and (5) holding people accountable for discharging their internal control related responsibilities. All five principles are essential to effective internal control over compliance.

- As with any objectives – be they operations, compliance or reporting – an evaluation of internal control begins with an understanding of the relevant risks. *Risk Assessment* requires objectives with sufficient clarity to enable the identification and assessment of the related risks. In identifying compliance objectives, Principle 6 requires consideration of applicable external laws and regulations, as well as management's tolerances for risk. Principle 7 deals with risk identification, and Principle 9 deals with the effects of change, both of which are highly germane to compliance management. If applicable, Principle 8 deals with the consideration of the potential for fraud when assessing risk.

- The risk assessment driven by the company's management provides a context for designing the *Control Activities* necessary to reduce risks to an acceptable level (Principles 10, 11 and 12). Note that Principle 10 deals with the selection and development of control activities that mitigate risk to the achievement of compliance objectives, and Principle 12 deals with the deployment of control activities through established policies and procedures. Principle 11 addresses the impact of controls over general technology to the extent they impact the achievement of compliance objectives.
- Regarding *Information and Communication*, the various principles are pretty broad (Principles 13, 14 and 15) and are readily adapted to compliance.
- *Monitoring* addresses the most critical controls, and Principles 16 and 17 are both germane to compliance.

In summary, all compliance-related risks and controls are driven off of the applicable external laws and regulations and management's tolerances for risks. While the 2013 New Framework is an adjustment for everyone, we believe that companies will find its application can be directed to compliance quite easily. With respect to interacting with regulators and external auditors, we recommend that companies take the lead in formulating their approach in applying the New Framework to compliance and be prepared to explain how and why their approach works. Every company is different, and COSO made it clear that professional judgment is required in applying the New Framework. For all public companies participating in the U.S. capital markets, their experience in evaluating ICFR in accordance with Sarbanes-Oxley Section 404 will help them apply the New Framework to other areas of compliance.

45. How does the New Framework relate to ERM?

COSO included Appendix G in the New Framework to address this question. In addition, the COSO 2004 *Enterprise Risk Management – Integrated Framework*, which established a framework for evaluating ERM, includes an appendix that addresses this topic.

The basic premise of the aforementioned appendices is as follows: ERM is broader than internal control and focuses more directly on risk. Internal control is an integral part of ERM, while ERM is part of the overall governance process. 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.

46. How does the new COSO framework align to COBIT 5?

Below is a graphic depicting the relationship between the two frameworks: The two frameworks are well aligned, with COSO providing a high-level structure and COBIT providing details to support management in developing specific controls.

	COSO Components				
COBIT 5 Domains and Processes	**Control Environment**	**Risk Assessment**	**Control Activities**	**Information & Communication**	**Monitoring Activities**
Governance					
Evaluate, Direct and Monitor					
EDM01 Ensure Governance Framework Setting and Maintenance	●		●		
EDM02 Ensure Benefits Delivery	●		●		
EDM03 Ensure Risk Optimization		●	●		
EDM04 Ensure Resource Optimization			●		
EDM05 Ensure Stakeholder Transparency	●			●	●
Management					
Align, Plan and Organize					
APO01 Manage the IT Management Framework	●		●	●	
APO02 Manage Strategy	●		●		
APO03 Manage Enterprise Architecture			●		
APO04 Manage Innovation			●		●
APO05 Manage Portfolio		●	●		
APO06 Manage Budget and Costs			●		
APO07 Manage Human Resources	●				
APO08 Manage Relationships	●			●	
APO09 Manage Service Agreements				●	●
APO10 Manage Suppliers			●	●	●
APO11 Manage Quality			●		
APO12 Manage Risk		●			
APO13 Manage Security		●	●		

	COSO Components				
COBIT 5 Domains and Processes	**Control Environment**	**Risk Assessment**	**Control Activities**	**Information & Communication**	**Monitoring Activities**
Build, Acquire and Operate					
BAI01 Manage Programs and Projects			●		●
BAI02 Manage Requirements Definition			●	●	
BAI03 Manage Solutions Identification and Build			●		
BAI04 Manage Availability and Capacity		●		●	
BAI05 Manage Organizational Change Enablement		●	●	●	
BAI06 Manage Changes			●		●
BAI07 Manage Change Acceptance and Transitioning			●		
BAI08 Manage Knowledge			●	●	
BAI09 Manage Assets		●	●		
BAI10 Manage Configuration			●		
Deliver, Service and Support					
DSS01 Manage Operations			●		●
DSS02 Manage Service Requests and Incidents			●		●
DSS03 Manage Problems			●		●
DSS04 Manage Continuity		●	●		
DSS05 Manage Security Services		●	●		
DSS06 Manage Business Process Controls	●		●		●
Monitor, Evaluate and Assess					
MEA01 Monitor, Evaluate and Assess Performance and Conformance					●
MEA02 Monitor, Evaluate and Assess the System of Internal Control					●
MEA03 Monitor, Evaluate and Assess Compliance with External Requirements				●	●

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 35 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 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

Contacts

Brian Christensen
Executive Vice President – Global Internal Audit
+1.602.273.8020
brian.christensen@protiviti.com

Jim DeLoach
COSO Subject-Matter Expert
+1.713.314.4900
jim.deloach@protiviti.com

Christopher Wright
Finance Remediation & Reporting Compliance Leader
+1.212.603.5434
christopher.wright@protiviti.com

THE AMERICAS

UNITED STATES

Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Denver
Fort Lauderdale
Houston
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
San Jose
Seattle
Stamford
St. Louis
Tampa
Washington, D.C.
Winchester
Woodbridge

ARGENTINA*

Buenos Aires

BRAZIL*

Rio de Janeiro
São Paulo

CANADA

Kitchener-Waterloo
Toronto

CHILE*

Santiago

MEXICO*

Mexico City
Monterrey

PERU*

Lima

VENEZUELA*

Caracas

ASIA-PACIFIC

AUSTRALIA

Brisbane
Canberra
Melbourne
Perth
Sydney

CHINA

Beijing
Hong Kong
Shanghai
Shenzhen

INDIA

Bangalore
Mumbai
New Delhi

INDONESIA**

Jakarta

JAPAN

Osaka
Tokyo

SINGAPORE

Singapore

SOUTH KOREA

Seoul

EUROPE/MIDDLE EAST/AFRICA

FRANCE

Paris

GERMANY

Frankfurt
Munich

ITALY

Milan
Rome
Turin

THE NETHERLANDS

Amsterdam

UNITED KINGDOM

London

BAHRAIN*

Manama

KUWAIT*

Kuwait City

OMAN*

Muscat

QATAR*

Doha

UNITED ARAB EMIRATES*

Abu Dhabi
Dubai

SOUTH AFRICA*

Johannesburg

* Protiviti Member Firm
** Protiviti Alliance Member

protiviti®
Risk & Business Consulting.
Internal Audit.