The Updated COSO Internal Control Framework

Frequently Asked Questions

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 – has released its long-awaited updated *Internal Control – Integrated Framework* (New Framework). 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 by public companies listed in the United States in accordance with Section 404 of the Sarbanes-Oxley Act. 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.

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 get started.

This 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. For interested parties, the New Framework is available at www.coso.org.

Protiviti

May 2013

Contents

Introduction i

1. Who is COSO? 1
2. How did the project to update the 1992 framework unfold? 1
3. How is the updated framework organized? 1
4. Why update the 1992 framework? 1
5. What hasn't changed? 2
6. What has changed? 3
7. What's the most important change? 4
8. How are points of focus applied? 6
9. How are deficiencies in internal control assessed? 10
10. What does "present and functioning" mean? 11
11. How does management assess whether all components "operate together"? 11
12. Are external parties a part of the system of internal control? 11
13. When are we required to apply the New Framework? 12
14. What if we continue to apply the original framework beyond COSO's transition period? 12
15. What are the implications for Sarbanes-Oxley compliance? 12
16. How do we disclose in our annual internal control report which framework we use during the transition period? 12
17. What do we need to do now? 13
18. What tasks are necessary in applying the 2013 New Framework? 13
19. To whom do we communicate – and what do we tell them? 13
20. Will there be a "street reaction" to companies that do not "early apply"? 13
21. Does the New Framework comment on the limitations of internal control? 14
22. How do we use the illustrative tools for assessing effectiveness of a system of internal control? 14
23. Why did COSO issue the Internal Control over External Financial Reporting: A Compendium of Approaches and Examples? 14
24. Are we required to use the External Financial Reporting Compendium? 14
25. How does the New Framework relate to ERM? 15

About Protiviti 16

1. Who is COSO?

The Committee of Sponsoring Organizations 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,[1] an applications guide providing illustrative tools, and a separate compendium of approaches and examples for application of the New Framework to internal control over financial reporting.

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 megatrend; 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 fiascos 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.

---

[1] 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.

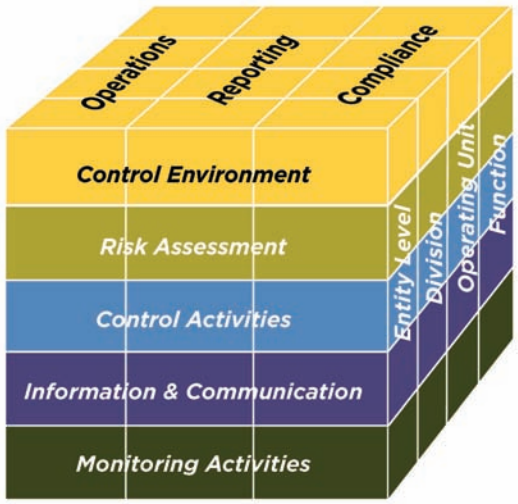
5. What hasn't changed?

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.[2] 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, the New Framework does not require separate evaluations of whether they 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 and 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.

---

[2] 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 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,[3] 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 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.

---

[3] 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,[4] as provided by the New Framework.

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

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
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
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			
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

Information and Communication (continued)			
Principles		**Points of Focus**	
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			
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 and specific circumstances.

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.

10. 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 director's oversight, needs to determine to what extent relevant principles underlying the component are present and functioning.

11. 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.

12. Are external parties a part of the system of internal control?

External parties, including external auditors and regulators, 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.

13. 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.

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

For companies complying with Sarbanes-Oxley, this would not be a wise choice. During the transition period, the COSO Board believes that application of its *Internal Control – Integrated Framework* that involves external reporting should clearly disclose whether the original or 2013 version was utilized. As noted above, there is a presumption that the 2013 New Framework will be used after the transition period expires. If it isn't, companies are likely to receive pushback from their external auditors – and perhaps from the SEC staff as well.[5]

15. 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 internal control over financial reporting. The latter compendium may be useful to companies complying with Sarbanes-Oxley.

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

In the internal control report, management must disclose the framework used as criteria for evaluating the effectiveness of internal control over financial reporting. 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.

---

[5] 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.

17. 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 early in 2013 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.

18. What tasks are necessary in applying the 2013 New Framework?

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 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. 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 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 next question).

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.

19. 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.

20. 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.

21. 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.

22. 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.

23. 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.

24. Are we required to use the 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.

25. How does the New Framework relate to ERM?

COSO included Appendix G in the New Framework to address this question. Rather than repeat all of the relevant points here, reference is made to this appendix. In addition, the COSO 2004 *Enterprise Risk Management – Integrated Framework*, which established a framework for evaluating ERM, includes an appendix that addressed 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.

About Protiviti

Protiviti (**www.protiviti.com**) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE 1000® and FORTUNE Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

About Our Financial Controls and Sarbanes-Oxley Compliance Practice

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

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

Our specific services include:

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

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

* Protiviti Member Firm
** Protiviti Alliance Member

EUROPE

FRANCE

Paris

GERMANY

Frankfurt
Munich

ITALY

Milan
Rome
Turin

THE NETHERLANDS

Amsterdam

UNITED KINGDOM

London

MIDDLE EAST

BAHRAIN

Manama*

KUWAIT

Kuwait City*

OMAN

Muscat*

QATAR

Doha*

UNITED ARAB EMIRATES

Abu Dhabi*
Dubai*

protiviti®
Risk & Business Consulting.
Internal Audit.

© 2013 Protiviti Inc. An Equal Opportunity Employer. PRO-PKIC-0513-106
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.