COSO 2013: WHAT HAS CHANGED & STEPS TO TAKE TO ENSURE COMPLIANCE

Experis™
ManpowerGroup

COMMITTEE OF SPONSORING ORGANIZATIONS (COSO) 2013

The Committee of Sponsoring Organizations (COSO) Internal Controls Integrated Framework, originally published in 1992, has certainly stood the test of time. Over the past two decades, the Framework has been used globally by public and private companies large and small, new and old. The COSO of the Treadway Commission recently issued an update to the Framework that reflects the multitude of changes since 1992 to business processes, information technology and corporate stakeholder expectations. The new Framework provides improved guidance for implementation, establishes a more effective internal controls structure, and improves corporate governance.

This paper summarizes the following:

1. An overview of the Framework
2. Key areas of emphasis within the new Framework
3. A proposed transition plan from the 1992 to the 2013 Framework

So, what has happened in the last 20 years to warrant this change?

- Dramatic changes in business and operating environments.
- Rapidly changing information technology systems and platforms.
- An increase in stakeholder sophistication relating to internal controls with the advent of Sarbanes-Oxley (SOX).
- Increased corporate expectations relating to the management of enterprise risk assessments.
- Reliance on third-party contractors to perform core business processes.
- Global expansion.
- Dramatic increases in the complexity of laws and regulations.
- Significant large scale and high profile breakdowns in controls.
- Drastic increases in global fraud, recently reported to be an estimated 3.2 trillion dollars.
- Global demand for improved management reporting.

The Public Company Accounting Oversight Board (PCAOB) also issued Staff Audit Bulletin Number 11 in October 2013, that addresses significant auditing practice issues observed by the PCAOB staff in the past few years relating to audits of internal controls over financial reporting. The practice alert revisits certain requirements of the internal control auditing standards of the

PCAOB in which significant auditing deficiencies have been cited frequently in PCAOB inspection reports. The Bulletin is having an impact on many areas, including the evaluation of the effectiveness of management level reviews.

Specifically, this recent Bulletin addresses the following topics:

- Risk assessment and the audit of internal control.
- Selecting controls for testing.
- Testing management review controls.
- Information technology ("IT") considerations, including system-generated data and reports.
- Roll-forward of controls tested at an interim date.
- Using the work of others.
- Evaluating identified control deficiencies.

The transition to COSO 2013 will mean different things to different organizations depending on the effectiveness and maturity of your system of internal controls over financial reporting. As a starting point, those impacted by COSO 2013 should consider purchasing the Framework either in hard copy or electronic format. In addition, COSO has released a number of publications that will further support this transition, including:

1. *Internal Control*—Integrated Framework Executive Summary. An overview of internal control, including a definition, categories of objectives, descriptions of the requisite components and associated principles, and requirements of an effective system of internal control.
2. *Framework and Appendices*—A detailed refresher of COSO, details around the principles and related points of focus, and additional considerations for developing your frameworks.
3. *Illustrative Tools for Assessing Effectiveness of a System of Internal Control*—Templates and illustrative tools to support your overall assessment of the system of internal control, component evaluation, principle evaluation, and addressing deficiencies.
4. *Internal Control over External Financial Reporting (ICEFR): A Compendium of Approaches and Examples*—Points of Focus, approaches and examples to provide guidance around applying the principles.

The Illustrative Tools for Assessing Effectiveness of a System of Internal Controls provides a template for demonstrating the required level of review and assessment necessary to evaluate an organization's level of compliance with the Framework.

OVERVIEW OF THE FRAMEWORK

To understand the basics of the Framework, it is necessary to understand the hierarchy structure of the Framework. Begin by reviewing the definition of internal controls:

"Internal control is a process affected 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."[1]

The Framework also sets forth **three categories of objectives**, that enable companies to focus on risks and controls at the enterprise level. The objective categories include:

1. Operations Objectives – pertain to the effectiveness and efficiency of the company's operations.
2. Reporting Objectives – pertain to internal and external financial and non-financial reporting.
3. Compliance Objectives – pertain to adherence to laws and regulations.

To support the efforts of the company to achieve its objectives, COSO has established **five components of internal control**. Specifically, these are:

1. Control Environment – Standards, processes, and structure that provide the overarching structure for carrying out internal controls.
2. Risk Assessment – Process for identifying and analyzing risks to achieving the company's objectives.
3. Controls Activities – Actions established by management policies and procedures to help ensure that management objectives to mitigating risks to the achievement of objectives are carried out.
4. Information and Communication – Information needed to carry out internal control responsibilities in support of management objectives.
5. Monitoring Activities – Evaluations used to determine whether each of the components is present and functioning.

The key enhancement to COSO 2013 is the introduction of 17 principles that provide a roadmap for the implementation and assessment of the internal control environment. They represent the fundamental concepts associated with each component (which have not changed). The principles within each component must be capable of being demonstrated to determine compliance with that component, and in turn the Framework (principles) must be "present and functioning." "Points of Focus" have been added that describe important characteristics associated with the principles. Embedded Approaches and Examples have also been added that describe how organizations may apply the principles.

[1] COSO publication: *Internal Control Over External Financial Reporting: A Compendium of Approaches and Examples*.

COSO CUBE 2013 EDITION

Since 1992, COSO has provided a layered view of the basic concepts of the Internal Controls Integrated Framework. The COSO cube has been updated to reflect the new Framework.

WHAT KEY AREAS DOES COSO EMPHASIZE IN THE NEW FRAMEWORK?

To understand the areas of emphasis within the new Framework, it is important to understand the 17 principles. They include the following:

PRINCIPLES OF EFFECTIVE INTERNAL CONTROL

CONTROL ENVIRONMENT	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
RISK ASSESSMENT	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
CONTROL ACTIVITIES	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
INFORMATION & COMMUNICATION	13. Uses relevant information 14. Communicates internally 15. Communicates externally
MONITORING ACTIVITIES	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

Control Environment

Depending on how they are viewed, the five principles within the Control Environment are either the wide foundation or the overarching umbrella of internal control. In short, this is the tone at the top established by the board of directors and senior management, and the reinforcement of expectations that have a pervasive impact on the overall system of internal control. It includes the organization's ability to demonstrate that they are following through with actions and not merely publishing policies once a year to check a box. It also includes the ability to demonstrate that the board of directors is independent from management and as part of their ongoing role, looking at internal controls and the performance of those controls. Finally, it includes the way in which the organization is designed—by unit and department, by the experience and depth of the people within the roles of the organization, and by the ongoing evaluation of performance and accountability against the organization's objectives.

Risk Assessment

The four principles associated with Risk Assessment address:

1. The clarity of objectives so that related risks are identified, analyzed, and managed, keeping in mind these principles are not limited to financial reporting objectives.
2. COSO emphasizes the need to take an enterprise view that focuses on all categories of risk, not just financial reporting risks.
3. Additionally, these principles require organizations to consider the potential for fraud in assessing risks to the achievement of objectives, and identify and assess changes that could impact the system of internal control.
4. Fraud risk assessment will be a significant area of emphasis by public accountants, the PCAOB and the SEC over the next few years.

Control Activities

The third component of internal control is Control Activities. These are the actions, established through policies and procedures, which help ensure management's directives are carried out for mitigating risks to the achievement of objectives. Control activities are performed at all levels of the entity, at various stages within business processes and over the technical environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews.

The key points of emphasis to consider include:

1. Are policies and procedures current and accurate, and do they include key controls?
2. Have the key technology risks been considered? Are they current and do they include all critical applications?

Information & Communication

The focus of the three principles related to Information and Communication is that organizations should obtain or generate and then use relevant, quality information to support the functioning of internal control. This includes communication within the organization at team meetings, dashboard, and other data or reports employed at all levels of management, to determine performance of internal control, evaluate the status of goals and objectives, and take action when needed.

These principles ensure that the responsibility for internal control is communicated internally—up and down the organization—and not simply reviewed by senior management. They also mandate communication with external parties regarding matters affecting the functioning of internal control. Reporting needs to consider four types of reports including internal financial, internal non-financial, external financial and external non-financial.

Monitoring Activities

The last two principles in the new Framework relate to the Monitoring Activities. Ongoing evaluations, built into business processes at different levels of the entity, provide timely information. Separate evaluations, conducted periodically, will vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Both types of evaluations must ascertain whether the components of internal control are present and functioning and the results of the evaluations must be communicated in a timely manner to those responsible for taking action. Action must be taken to address the items noted in the evaluations.

WHAT TO CONSIDER WHEN TRANSITIONING TO COSO 2013?

Based on Experis' experience in performing hundreds of engagements in many industries, we would like to share some important considerations for a SOX model for transitioning from the 1992 to the 2013 Framework. Please note that the process defined below is an iterative one that requires repetition until it is perfected.

There are FOUR STEPS in the process:

1. Building internal awareness and expertise.
2. Performing an impact assessment and preparing the project plan.
3. Executing the transition plan.
4. Engaging, communicating with, and training key stakeholders.

COSO 2013: SOX TRANSITION METHODOLOGY

Build Internal Awareness & Expertise

- Build awareness
  - Obtain COSO publications
- Revisit concepts & definitions
  - Internal control definition
  - Categories of objectives
  - Control components
  - Entity structure
  - Management judgment
- Understand the principles
  - Principles (17)
  - Points of focus (81)
  - Approaches
  - Examples
- Understand definition of effective internal control
  - Present & functioning
- Understand the definition of internal control deficiencies

Perform Impact Assessment/ Prepare Project Plan

- Revisit existing controls documentation to determine adequacy
  - Financial reporting objectives
  - Risk assessments
  - Significant accounts / disclosures
  - Assertions
  - Processes & transactions
- Define the project plan & methodology
  - Finalize methodology & approach
  - Define the project team
  - Develop the project plan

Execute the Transition Plan

- Documentation & valuation
  - Map the principles & components (Using points of focus, approaches, & examples) to the existing documentation
- Confirm existing understanding with control owners
- Control design evaluation & gap remediation
  - Evaluate the control design
  - Define gaps
  - Remediate identified gaps
- External review
  - Coordinate with external auditor

Engage, Communicate & Train

- Engage broader organization
- Communicate with key stakeholders
- Perform training

OVERALL PROJECT MANAGEMENT

STEP ONE: DEVELOP AWARENESS, EXPERTISE, AND ALIGNMENT

In addition to obtaining executive leadership support, the first step in transitioning to COSO's 2013 Framework is to build an internal awareness and expertise among resident COSO and SOX subject matter experts. In other words, it is important to revisit the basics.

As noted earlier, COSO has released a number of publications that will support this transition.

Codified Principles

The old Framework conceptually introduced the concepts associated with the five components of internal control. Because the new concepts are essential to assuring that the five components are present and functioning, these concepts are now explicitly articulated in the 17 principles and 81 points of focus. The Framework describes Points of Focus to assist management in designing, implementing, and maintaining internal control, and in assessing whether the 17 principles are present and functioning. Points of Focus represent important characteristics of the principles. Additionally, approaches are provided that describe how organizations may apply the principles. Examples are given to provide specific illustrations on the application of each principle. Tools and templates to help map a controls framework are available within the publications discussed earlier.

For example, principle one states the organization should demonstrate a commitment to integrity and ethical values.

Supporting Four Points of Focus

1. Setting the tone at the top
2. Establishing standards of conduct
3. Evaluating adherence to standards of conduct
4. Addressing deviations in a timely manner

Requirements of Effective Internal Control

For management to conclude that its system of internal control is effective, all five components of internal control and all relevant principles must be present and functioning. Being "present" implies a given component or principle exists within the design and implementation of an entity's system of internal control. "Functioning" implies the component or principle continue to exist in the operation and conduct of the control system. Effective internal control also requires that all five components operate together in an integrated manner. "Operating together" refers to the determination that all five components collectively reduce the risk of not achieving an objective.

Internal Control Deficiencies Definition

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

STEP 2: PERFORMING AN IMPACT ASSESSMENT AND PREPARING THE PROJECT PLAN

Like most organizations, once the original methodology and approach for SOX compliance was developed, the entity most likely invested significant time up front to define an internal control framework, starting with COSO's old Framework and then customizing it based on the organization's specific processes, financial disclosures and risk history.

First, a high-level financial reporting objective was probably specified related to preparing financial statements and disclosures. In doing so, significant financial statement accounts were identified based on the risk of material misstatement. Then, for each account or disclosure, relevant financial reporting assertions were identified. In addition, underlying transactions, events, and processes supporting the respective accounts and disclosures were also identified. The result may have been a mapping of the design of the organization's internal control environment, providing evidence that control activities are in place for all relevant financial reporting assertions and for all significant accounts and disclosures. If there were any major gaps, they were remediated accordingly.

Assuming an organization went through such a vigorous process in developing the existing SOX compliance program, the organization can now leverage the original mapping to determine the impact of the transition to the new Framework. Now, however, instead of mapping directly to the five components of internal control, first map to the 17 principles that underlie each of the five components. As before, if it is determined there are gaps in the internal control design, it will be necessary to remediate them accordingly.

The organization's updated SOX compliance methodology and approach will be finalized during this phase, in addition to defining project governance and decision rights, developing a detailed project plan with key milestones, identifying and assigning resources, and completing other necessary planning activities. Even those companies with sophisticated SOX compliance programs today who have designed, implemented, and maintained effective systems of internal control will need to expend some effort in the transition.

The following are both tactical and strategic questions for consideration.

Tactical Questions:

- What has our recent experience been relating to our SOX program?
- Where have we had past issues relative to control deficiencies?
- What have we learned from these past experiences?
- How current is our internal control documentation?
- How well developed are our risk management and internal control processes?
- Who owns the system of internal controls?
- How engaged is management and senior management in owning the system of internal controls?
- What opportunities do we have to improve the internal control structure?
- What is the level of understanding of the audit committee and board?

Strategic Questions:

- Will our focus be on ICFR, or will we more broadly apply the Framework to compliance, operations and non-financial reporting?
- How have key business decisions impacted our risk profile/control environment?
- Can the control environment absorb complex change—globalization, finance transformation, technology?
- Do we have sufficient resources to support the control environment or anticipated changes to the business?
- How do we leverage implementation to improve dialogue around risk and controls and the business unit ownership?
- How do we leverage implementation to improve overall stakeholder dialogue around risk and controls?

STEP 3: EXECUTING THE TRANSITION PLAN

Once the organization has built broad awareness regarding the updated COSO Framework, gained senior leadership alignment and support that a timely transition is important, and completed a comprehensive impact assessment and project plan, it is time to develop and execute a transition plan.

As the transition plan is executed, Experis Finance recommends three high-level phases:

Phase 1: Documentation and Evaluation

During this phase, the organization may need to update the format and/or flow of underlying documentation. Specifically, for management to conclude that its system of internal control is effective, all five components of internal control and all relevant principles must be present and functioning. The underlying documentation must support management in making such a conclusion. Again, COSO provides publications with tools and templates that can help facilitate this process.

This phase also entails evaluating the design of the underlying controls and enhancing the design as needed. It is also very important to communicate with the control owners to ensure they are on board with the plan.

Phase 2: Control Design Evaluation and Gap Remediation

First, spend time understanding and evaluating the controls design. Many companies take advantage of this time to optimize and/or rationalize their controls. Removing redundant, duplicate and non-value-added controls is important to ensure that maximum efficiency exists within your controls framework.

Once the design effectiveness of your internal control structure has been evaluated, it is important to remediate any gaps identified.

Phase 3: External Review

At some point, the external auditor will need to assess and gain comfort with the updated SOX compliance program and supporting documentation. Be sure to spend time with your auditors, who are under extreme pressure based upon the PCAOB recently issued Staff Audit Practice Alert No. 11.

Maintaining close alignment with auditors will help to ensure there are no surprises.

STEP 4: ENGAGING, COMMUNICATING WITH AND TRAINING KEY STAKEHOLDERS AND CONSTITUENTS

In step four, it is time to facilitate broad awareness of COSO's updated Framework and the potential impact on your SOX compliance program among key stakeholders, including the board of directors/audit committee, senior and operational management, process and control owners, and internal auditors. Be sure to discuss the impact of COSO's 2013 Framework on SOX efforts with the organization's external auditors, as mentioned before. In some cases, in-depth training may be appropriate for all stakeholders.

In addition to building broad awareness, have those who are directly responsible for implementing the company's SOX controls critique the preliminary mapping to ensure the analysis is complete and accurate.

What Else Do You Need to Know?

- The original Framework will remain available and has been deemed appropriate for use through December 15, 2014.
- The SEC staff plans to monitor the transition for public issuers who continue to use the 1992 Framework after December 15, 2014, to evaluate whether and if any staff or Commission actions become necessary or appropriate at some point in the future.
- The SEC announced its examination priorities for 2014. These include a focus on fraud detection and prevention, corporate governance, enterprise risk management, technology controls, retirement investments, and issues posed by the convergence of broker-dealer and investment adviser businesses.

If you have any questions or would like to discuss how to start evaluating your organization against the COSO 2013 Framework, contact an Experis Finance representative. We have a team of professionals experienced in working with organizations to ensure compliance with the new principles. Learn more about us at Experis.us/finance.com.

EXPERIS
100 MANPOWER PLACE
MILWAUKEE, WI 53212
USA
WWW.EXPERIS.COM