Lessons from the Front Line on COSO 2013
COSO 2013

Agenda

• Overview of the COSO Framework
• COSO Implementation Now or Later?
• COSO Mapping Objectives and Key Steps
• What we are Seeing as Key Focus Areas and Results
• Tips to Surviving COSO 2013
The COSO Framework sets forth three categories of objectives that enable companies to focus on risks and controls at the enterprise level. The objective categories include:

- **Operations Objectives** – pertain to the effectiveness and efficiency of the company’s operations
- **Reporting Objectives** – pertain to internal and external financial and non-financial reporting (**Sarbanes-Oxley Requirements**)  
- **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:

<table>
<thead>
<tr>
<th>5 Components of Internal Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Control Environment</td>
</tr>
<tr>
<td>2. Risk Assessment</td>
</tr>
<tr>
<td>3. Control Activities</td>
</tr>
<tr>
<td>4. Information and Communication</td>
</tr>
<tr>
<td>5. Monitoring Controls</td>
</tr>
</tbody>
</table>
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 provided that describe how organizations may apply the principles

*Note – All principles must be present and functioning to support a well designed Sarbanes-Oxley compliance program but not all points of focus relate to Internal Control Over Financial Reporting*
### COSO 2013

**KEY AREAS COSO EMPHASIZES IN THE NEW FRAMEWORK**

#### PRINCIPLES OF EFFECTIVE INTERNAL CONTROL

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

- Implementation due by December 15, 2014

- KPMG recently suggested clients may not want to implement by December 15, 2014 (see Compliance Week article “Buying Time on COSO’s Internal Control Framework Update”, published on July 29, 2014)

- The Securities and Exchange Commission says companies are required to use a “suitable” framework, but they haven’t explicitly said they would consider the 1992 framework unsuitable.

- Where’s the potential rub?
  - Clients must disclose they have not implemented the new framework
  - Further, they must disclose why – article points to the following as a good excuse:
    
    “Significant merger or acquisition activity”
    
  - Article also points out “if companies decide not to adopt the framework this year, it will be important to communicate it to auditors so they can test controls accordingly.” Could result in increased audit costs
COSO Implementation Now or Later?

• Hearing otherwise from other firms – “Deloitte fired a warning shot that when a company decides to stick with the expired framework for another year, the auditor should note that in their audit report”

• May be a case where disclosure is “we are partially complete in the conversion to the new framework”
Objective COSO 2013 Assessment

Evaluate the five components of internal control, including the 17 underlying principles and related entity-level and transaction-level controls to determine if the entity has effective internal control over external financial reporting.
Key Steps to Implementation

1. Map Existing RCM to COSO Framework
2. Verify the Design of the Controls
3. Address the Principles and POF
4. Summarize Changes/Gaps for Review with Management and Others
5. Gain Approval
6. Update Test Scripts and Process Documentation
7. Test
Key Focus Areas:

- **Board, Committee and Senior Management’s roles and responsibilities** for establishing and communicating effective standards, processes and structures as the basis for carrying out and holding individuals accountable for internal controls across the organization
- Establishing an **anti-fraud program and controls** that address the risks of material misstatement due to fraud
- Communication of expected ethical **values and code of conduct** to internal and **external** third parties
- **Completeness and accuracy** of the information used in the execution of the controls by the control owner
- **Level of precision** in the design and execution of controls, particularly management review controls
# KEY COSO PRINCIPLES AND POF TARGETED TO BOD AND MANAGEMENT

<table>
<thead>
<tr>
<th>COSO Principle - Control Environment</th>
<th>Points of Focus targeted to BOD and Management</th>
</tr>
</thead>
</table>
| #1 - The Organization demonstrates a commitment to integrity and ethical values | 1. Sets the tone at the top  
2. Establishes and communicates clear standards of conduct (integrity and ethical values)  
3. Processes in pace to evaluate compliance with expected standards  
4. Addresses deviations from expected standards in a timely manner |
| #2 - The BOD demonstrates independence from management and exercises oversight of the development and performance of internal controls | 1. BOD identifies and accepts its oversight responsibilities  
2. BOD defines, maintains, and periodically evaluates member skills needed to perform oversight responsibilities  
3. BOD has sufficient members to operate independently from management  
4. Provides oversight for system of Internal controls |
| #3 - Management established, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives | 1. Consider structures used to support the achievement of objectives  
2. Management establishes appropriate reporting lines with BOD oversight  
3. Defines, assigns, and limits authorities and responsibilities |
### KEY COSO PRINCIPLES AND POF TARGETED TO BOD AND MANAGEMENT

<table>
<thead>
<tr>
<th>COSO Principle - Control Environment</th>
<th>Points of Focus targeted to BOD and Management</th>
</tr>
</thead>
</table>
| **#4 -** The Organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives | 1. Establishes policies and procedures  
2. Evaluates competencies across the organization and addresses shortcomings  
3. Attracts, develops and retains sufficient and competent personnel and outsource providers to achieve objectives  
4. Plans and prepares for succession important to internal control |
| **#5 -** The organization holds individuals accountable for their Internal controls responsibilities in the pursuit of the objectives | 1. Enforces accountability for internal control through structures, authorities and responsibilities  
2. Establishes performance measures, incentive and rewards  
3. Periodically evaluates performance measures, incentives and rewards for ongoing relevance  
4. Considers excessive pressures associated with meeting objectives  
5. Evaluates performance of internal control responsibilities and rewards or disciplines individuals |
Results – What we are Seeing

• Time consuming to make the process “value add” versus a check the box exercise. POF appear similar at first glance, but important to:
  • Evaluate POF in the context of the Principle when evaluating the related controls
  • Assign several controls under each POF to prevent a single point of failure

• Significant portion of the framework covered by existing business and IT process controls

• Enhanced wording required of many of the organization’s entity level controls to encompass the intent of COSO’s principles and points of focus

• A dozen or more new controls added with half that many existing just not previously documented

• All of the big four COSO templates drive to the same answer but all in different ways

• Potential deficiency where POF’s required in support of the principle are not addressed

• A need for education of Board and Audit Committee members regarding their roles and responsibilities
Tips for Surviving COSO 2013

• Gain sponsorship by Senior Management. Meet early and often, with management, externals, get buy off on approach and new controls and changes to existing control language
• Consider how changes will impact the 302 certification process
• If mapping to POF use one document preferably in the format required by the external auditors
• Review your risk and controls carefully to ensure they address the intent of the POF
• Utilize a team approach for the mapping process
• Negotiate and get agreements on deviations from suggested approach by the external audit firm in writing
• Use the COSO tools especially the Compendium of Approaches and Examples
• Make all changes in RACM, utilize a tool such as vlookup to populate the COSO 2013 template
Questions?

Christine Bellino, CPA
Director, Risk Advisory Services
Experis Finance
720-663-8469
Appendix – IPEs and MRCs
Completeness and Accuracy

- What is an Information Provided by Entity (IPE)?
  
  - PCAOB Auditing Standard No. 15 states that, in order to obtain reliable audit evidence, information produced by the entity (“IPE”) that is used for performing audit procedures needs to be sufficiently complete and accurate.

  - Per COSO 2013 - Principle 13: The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

  - When using IPE produced by the company as audit evidence, the auditor should evaluate whether the information is sufficient and appropriate for purposes of the audit by performing procedures to:
    - Test the accuracy and completeness of the information, or test the controls over the accuracy and completeness of that information
    - Evaluate whether the information is sufficiently precise and detailed for purposes of the audit.
Completeness and Accuracy

• Types of IPE
  – There are two types of IPE:
    ◦ A Population IPE is a report that identifies the population subject to a control
    ◦ An Execution IPE is a report that is relied upon by the client when performing a control
  – IPEs apply to both business process and IT controls

• Examples of IPEs
  – List of new hires from the HR or Payroll system
  – List of approved invoices
  – A/R Aging
  – Password Parameter Settings
  – Month-to-Month Management Reports
  – Queries
  – Spreadsheets
IPEs – Reminders

• Emphasis should be on the identification, documentation, and verification of IPEs as part of the control procedures. This may be a significant change for many organizations.

• PBC (Provided By Client) requests need to specify the reports required for population testing as well as control testing and the timing of when these should be run/observed.

• Observing population generation can create scheduling problems - people have to be available to run reports and provide screen prints while you watch.

• Meet with the external audit team prior to the start of field work to coordinate audit efforts, timing, and approach to IPE testing and their reliance strategy.
Review Log of IPEs and Links to IT General Controls

ITGCs – Access and Change Management, Interfaces

SAP General Ledger

SAP Inventory

Data Warehouse

Interfaces

Manual Control

Journal to record reserve adjustment

Report of inventory items with last transaction dates and volumes

Slow moving reserve spreadsheet with calculations and filters

IPEs
Management Review Controls (MRCs)
Overview

• Component of COSO 2013

• May be higher level or process level controls

• Normally involve a manager reviewing one or more of:
  – Reports or other IPEs
  – Variance reports
  – Exception reports
  – Detailed calculations supporting financial statement balances or disclosures
  – Assumptions involving significant management estimate or judgment

• Documentation should address how the design and operation addresses all relevant WCGWs

• External auditors will determine level of risk by assessing:
  – Degree of judgment involved – this will also be apparent from the types of relevant assertion
  – Whether control is within the process or whether it monitors effectiveness of other controls
MRC Themes

- **Specificity of Scope/Precision** – defining materiality/significance and including thresholds - avoid “material” or “significant” and define thresholds

- **Specificity of review** – details of what reviewer looks for and what constitutes an outlier or exception

- **Exceptions** – follow up and resolution with applicable evidence – need to define what an exception is

- **Physical Evidence** – evidence of performance of control – inquiry and calendar invites are not sufficient – need meeting minutes detailing discussion points/action items with evidence of follow up. Signed and dated review, reconciliation etc. with evidence of tie-outs or tick marks, checklist with sign-off details with exceptions noted

- **IPEs** – management validation over completeness and accuracy of data and reports used in performance of controls
A matrix for each new leased property will be completed during the monthly close by the Senior Financial Reporting Analyst, Assistant Controller, or Controller. Each matrix requires a review by a second member of the accounting team, the Senior Financial Reporting Analyst, Assistant Controller, or Controller. The reviewer will ensure that the matrix has been correctly completed and all relevant criteria have been properly assessed in the determination of whether the lease is capital or operating. The review will address all sections of the matrix and ensure that:

- Lease terms (including possession date, rent, any escalations, tenant allowance, and term) are in accordance with current lease documentation
- Consideration is given for tenant’s involvement during construction
- Fair values are supported by independent data
- Four lease classification tests have been completed where appropriate
- Lease incentives have been addressed
- Conclusions are supported by the documented facts

Any anomalies or issues identified in the review are documented and resolved before the matrix is approved. Evidence of who performed the review and the timing will be included in a tab within the matrix.