COSO 2013/SOX – Lessons Learned and What’s Next

George W. Graves
May 13, 2015
The Current SOX Environment Driving the Need for Change
The Current Environment

Today companies are facing:

- Last minute ‘crises’ due to late demands from auditors
- Low perceived value of SOX programs
- Increased cost of compliance and last minute overages
- The need to adopt COSO 2013
- Spike in turnover of SOX/internal audit teams
- Pressure to keep SOX programs pushed down as far as possible
- Challenge to keep up with rapidly evolving expectations from the PCAOB/SEC/COSO
- Desire to increase auditor reliance to reduce external audit fees

- Management is struggling to maintain control over their SOX programs in the face of increased regulatory scrutiny and demands from their external auditors and regulators.
- It is time for management to focus more on effective and efficient processes and controls to ultimately lower risk and cost.
Relationship Among COSO Components

CONTROL ACTIVITIES

Process level activities, WCGWs, Controls that **directly** impact financial statement assertions

- Control Environment
- Risk Assessment
- Information and Communication
- Monitoring Activities

Indirect Entity Level Controls

Standards, Processes, Structures, Mechanisms… and Controls
Top 10 Areas Requiring Additional Effort

1. Apply the principles and points of focus across the organization and at all levels, including Third Party Service Providers (begins with Principle #1)

2. Board oversight (Principle #2)

3. Align performance management system with internal control responsibilities (Principle #5)

4. Determine materiality and risk tolerance for business units and controls at business process level (Principles #6 and 10)

5. Integrate conduct of business/operational risk assessment and monitoring with ICOFR risk matrix (Principles #7 and 9)

6. Conduct entity-wide fraud risk assessment to determine sufficiency of fraud risk controls (Principle #8)

7. Link general IT controls to related application controls and business processes (Principles #10 and 11)

8. Establish a process for identifying information needs and sharing relevant, timely information internally and externally (Principles #13, 14 and 15)

9. Establish monitoring activities in business processes and components (Principles #12 and 16)

10. Documentation

Demonstrate that the 17 principles and five components are present and functioning and that the components work in an integrated manner
2013 COSO Framework Transition Impact

### High Impact to Organization

- Limited planning & scoping process and documentation
- Multiple locations
- No fraud risk assessment
- Limited/weak/non current SOX documentation
- Unclear processes
- Heavy reliance on transaction controls
- Decentralized process
- Unclear accountability over controls
- No/limited reporting to management and board
- High level of turnover. Limited change management
- No/limited training provided to employees regarding controls, PCAOB trends, etc.
- Limited IT governance
- No clear correlation between ITGC and other controls
- Disparate systems or homegrown systems
- Constant control failures and remediation
- High reliance on many spreadsheets
- Decreasing investment in SOX

### Little Impact to Organization

- Robust and scalable planning & scoping process and documentation
- Fraud risk assessment
- Robust SOX documentation
- Well defined processes
- Balanced controls portfolio that identifies both material and non-material errors
- Centralized process
- Accountabilities embedded throughout the organization appropriately
- Defined metrics and good reporting to management and board
- Limited turnover and good change management in place
- Annual training provided to employees regarding controls, PCAOB trends etc.
- Robust IT governance
- Clear correlation between ITGC and other controls
- Common ERP systems
- Very few spreadsheets
- Maintained or increased investment in SOX compliance
What additional effort is required to improve your documentation of ICOFR?

- No incremental effort: 4%
- Some incremental effort: 56%
- Significant incremental effort: 19%
- Not sure: 21%

Documentation of existing and enhanced processes and controls is expected to be one of the main areas of additional effort when transitioning to COSO 2013.
Consider the following regarding the transactions or information processed by TPSP:

- The significance of the transactions processed by the TPSP to the entity’s financial statements
- The risk of a material misstatement due to error or fraud associated with the transactions processed by the TPSP
- The nature and complexity of services provided by the TPSP
  - How unique or highly standardized are they?
- Extent of delegation of authority to the TPSP
- How do the entity’s processes and controls interact with those of the TPSP?
- Is the TPSP part of the entity’s IT systems?

Consider applicability of 5 components and 17 principles
# COSO 2013 “Adoption” Observations

<table>
<thead>
<tr>
<th>Component</th>
<th>Observation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Activity</td>
<td>Companies who believed they were good at COSO 2013 and struggled with information produced by the entity (IPE) and MRCs, truly didn’t get COSO 2013. The concepts of IPE and MRCs are embedded in the principles and points of focus and the SEC Release No. 33-8810.</td>
</tr>
<tr>
<td>Monitoring</td>
<td>If auditors identify a deficiency before the company, the company has a problem. If auditors find more than the company, the company has a problem. If auditors find significant deficiencies or material weaknesses and the Company doesn’t, the Company has a problem.</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>If you can’t easily articulate the most likely causes of a material misstatement AND what controls you specifically test to address, then you likely have a problem.</td>
</tr>
<tr>
<td>Control Environment</td>
<td>If all your Board of Directors involvement with ICOFR is a short debrief of the outcome then it’s hard to see how you got Principle 2 right.</td>
</tr>
<tr>
<td>Control Environment</td>
<td>If the Company has only one person who has read the Framework and understands the theory, they are probably being driven by the auditor…a bad outcome.</td>
</tr>
</tbody>
</table>
A Robust Risk Assessment Process Helps Optimize Management’s Internal Controls
Using a Top-Down Risk Based Approach

Key benefits to a top-down risk-based approach to assessing financial statement risk:

- Drives a consistent approach to assessing financial statement risk across the organization
- Enables deployment of resources towards areas of higher risk and priority while allowing for customization to organizational needs
- Identifies low-risk areas where direct assessment may be replaced with enhanced certifications
- Aligns project approach to applicable laws, guidance, and precedents set by governing authorities and standard setting bodies (including the PCAOB, COSO, COBIT, and the SEC)
- Allows for controls rationalization – the “right” controls not just more or less
- Creates a defensible position for management’s 404(a) certification

Inherent Risk Assessment
Identify risks to financial reporting elements considering qualitative and quantitative factors. Map identified risks to financial statement assertion level

Entity-Level Control ("ELC") Review and Assessment
Evaluate high-level company-wide controls related to control environment, risk assessment, information & communication, and monitoring

Residual Risk Assessment
Evaluate the design and precision of entity-level controls and determine remaining financial statement assertion risk

Controls Rationalization/Key Control Identification
Identify relevant monitoring and process-level controls based on level of residual risk

Testing Approach
Develop testing approach which is generally a combination of entity-level and process-level control

Control framework to support adequate ICOFR are in place.
Risk Assessment Maturity

Where are you in the risk assessment and scoping maturity spectrum?

<table>
<thead>
<tr>
<th>Element</th>
<th>Basic</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Assessment</td>
<td>■ Risk Assessment is rolled forward annually by lower level employees that don’t understand how GAAP applies to the company</td>
<td>■ Individuals involved in the Risk Assessment have a strong understanding of GAAP and how it applies to the company</td>
</tr>
<tr>
<td></td>
<td>■ Overall risk ratings are assigned to the financial statement line items but not to specific assertions</td>
<td>■ Specific assertions (completeness, existence, valuation, rights and obligations, presentation) are linked to each consolidated financial statement line item (financial statement amounts) and related disclosures (collectively, financial reporting elements)</td>
</tr>
<tr>
<td></td>
<td>■ Fraud risk is considered at the financial statement line item</td>
<td>■ Fraud-risk identification and assessment, broad programs and controls related to fraud are considered in addition to controls that address specific fraud risks</td>
</tr>
<tr>
<td></td>
<td>■ Plan and scope based on financial statement coverage (Assets or Liabilities)</td>
<td>■ Both qualitative and quantitative sources of potential risk are considered when evaluating the potential likelihood of misstatement at the assertion level</td>
</tr>
<tr>
<td></td>
<td>■ Auditor drives scope based on financial statement coverage and prior year’s results</td>
<td>■ The design and operating effectiveness of the direct ELCs are considered to drive down the residual risk at the assertions level</td>
</tr>
<tr>
<td></td>
<td>■ Direct ELCs are not considered during the risk assessment</td>
<td>■ Locations are scoped based on their associated risk</td>
</tr>
<tr>
<td></td>
<td>■ Compliance efforts are not typically linked to scope</td>
<td>■ Testing is only completed in those locations that are not sufficiently covered by company level controls</td>
</tr>
<tr>
<td></td>
<td>■ Separate risk assessment and location testing plan with limited reliance</td>
<td>■ Testing and executing too many controls relative to risk</td>
</tr>
<tr>
<td></td>
<td>■ Testing is executing too many controls relative to risk</td>
<td>■ Risk Assessment is rolled forward annually by lower level employees that don’t understand how GAAP applies to the company</td>
</tr>
</tbody>
</table>

**Decreased Reliance on Process-Level Testing**

**Increased Effectiveness & Efficiency**
The Case for Deriving Value from SOX Programs
## Reliance Should Be a Deliberate Economic Decision

<table>
<thead>
<tr>
<th>Company's Regulator</th>
<th>External Auditor's Regulator</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SEC</strong></td>
<td><strong>PCAOB</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Less Auditor Reliance</strong></td>
<td><strong>More Auditor Reliance</strong></td>
</tr>
<tr>
<td>Information Provided by the Entity (IPE)</td>
<td></td>
</tr>
<tr>
<td>Increase in physical evidence required to support control</td>
<td>Enhanced, detailed audit procedures particularly around management review controls</td>
</tr>
<tr>
<td>More specificity around review controls</td>
<td>Level of precision, documentation around what attributes are reviewed for vis-à-vis expectations</td>
</tr>
<tr>
<td>More testing later in the year</td>
<td>Guidance around timing of testing (interim and rollforward) and sample sizes for each</td>
</tr>
<tr>
<td>Depth of Testing</td>
<td>Larger sample sizes, particularly for high risk controls and test procedures that dig deep</td>
</tr>
</tbody>
</table>

- Completeness and accuracy should be considered for key spreadsheets and system generated reports. GITC baseline key to reducing effort
- A variety of methods employed to test control effectiveness
- Role of management's judgment plays a critical role in determining design of controls and how they are evidenced
- More flexibility in determining how much to test and when.
- No sample size requirements (although most use external auditor guidance) and judgment on procedures

---

© 2015 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. NDPPS 334776
Companies with a strong process and control culture tend to perform better.
Controls Integration

**Fragmented State**: Compliance is project-centric. It is achieved through disconnected and/or inconsistently applied efforts throughout the enterprise.

**Functional State**: Compliance is program-centric. It is achieved via the oversight of a new, overarching, stand-alone program that oversees the hiring of dedicated personnel whose main focus is coordinating and communicating the compliance activities.

**Integrated State**: Compliance is process-centric. It is achieved in a fundamentally new way by building compliance activities and procedures into existing business processes and technology so that business owners can start to share responsibility for compliance.

**Embedded State**: Compliance is culture-centric. It is achieved as part of how business is done and is inherently part of organizational culture.
# The SOX Continuum – Where Do You Fall?

<table>
<thead>
<tr>
<th>Focus Areas</th>
<th>Basic</th>
<th>Mature</th>
<th>Advanced</th>
<th>Desired State Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Assessment</strong></td>
<td></td>
<td></td>
<td></td>
<td>- Establish risk-based scoping methodology using quantitative and qualitative factors (COSO 2013 – Principle 6)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Must reflect the entity’s structure and culture with a mechanism for updating for change</td>
</tr>
<tr>
<td><strong>Entity-Level Controls</strong></td>
<td></td>
<td></td>
<td></td>
<td>- SOX documentation (preferably control matrices and flowcharts) should exist for all processes</td>
</tr>
<tr>
<td>and Control Selection</td>
<td></td>
<td></td>
<td></td>
<td>- SOX documentation should be up-to-date for the current fiscal year</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Leverage Direct and Monitoring ELCs to reduce transaction-level testing</td>
</tr>
<tr>
<td><strong>Testing Approach</strong></td>
<td></td>
<td></td>
<td></td>
<td>- Leverage IT application controls to reduce manual control testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Implement risk-based testing approach</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Test procedures should be clearly mapped to the risk and control design</td>
</tr>
<tr>
<td><strong>Project Management/Governance</strong></td>
<td></td>
<td></td>
<td></td>
<td>- Audit Committees are proactive in overseeing SOX programs and managing the external auditor.</td>
</tr>
<tr>
<td>Structure</td>
<td></td>
<td></td>
<td></td>
<td>- Define and communicate roles and responsibilities for Internal Audit, Corporate, functional leaders and process owners, including executive sponsorship</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Establish SOX Playbook, including training and policy for process and control owners</td>
</tr>
</tbody>
</table>

© 2015 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. NDPPS 334776
Current PCAOB ICOFR Focus Areas

The risk assessment, planning and scoping process allows management the framework necessary to make decisions around some recent PCAOB focus areas that have significantly impacted the scope of SOX efforts

- Management Review Controls (MRCs)
  - **Specificity of Scope/Precision** – Defining materiality/significance and including thresholds
  - **Specificity of Review** – Including comprehensive details of what reviewer looks for during review and defining what constitutes an outlier/exception. Follow-up on variances, inconsistencies, and outliers
  - **Physical Evidence** – Physical evidence of the performance of a control is required (e.g., retain emails, etc. to evidence follow-up and resolution)
  - **Information Provided by Entity (IPE)** – Management validation over completeness/accuracy of data and reports used in performance of controls

- Increased Focus on Process Areas (i.e., identified revenue as one of the most common areas for audit deficiencies)
- System Interfaces – Additional validation required from both business and IT
- Risk Factors – Additional documentation and testing
- Reliance on Work of Others – Must pass PCAOB standards
- COSO 2013 – 17 principles present and functioning
Upcoming PCAOB ICOFR Focus Areas

- **Merger and acquisition** activity, including controls around business combinations and testing of cash flow projections used to support valuations;
- **Income taxes**, including controls over undistributed earnings and cash held overseas;
- **Investment returns**, including valuation of financial instruments, particularly hard-to-value securities;
- **Falling oil prices**, including considering the effects and the associated audit response;
- **Statement of cash flows**, in view of increasing errors in cash flow statements in areas considered to be less complex in nature;
- **Data and analytics tools**, particularly engagement teams’ understanding of how to use big data in an audit and developing professional skepticism when employing these tools;
- **Cyber security risks**, including how engagement teams consider these risks in the audit; and
- **Broker-dealer** auditing and attestation standards.
Next Steps – Questions to Ask Yourself

■ Where do you stand with respect to the SOX Maturity continuum?
■ How does your SOX program align with your broader compliance program?
■ How integrated is your IT function into the process?
■ Have you considered how technology can enhance your control portfolio?
■ Has your planning process been communicated to and aligned with your external auditor?
■ When was the last time the Finance and IT function received control training?
■ When was the last time you conducted a SOX Healthcheck on your program?