The New COSO Framework: Avoiding Deficiencies and Driving Change

Wednesday, August 12, 2015: Geek Week
Speaker Introductions

Kimberley Mobley, CPA, CISA
Partner
kmobley@johnsonlambert.com

Jill Cleaveland, CISA
Senior Manager
jcleaveland@johnsonlambert.com

Greg Daniel, CISA, CRMA
Manager
gdaniel@johnsonlambert.com
Presentation Overview

• Why update the original framework?
• What is changing?
• New areas of emphasis
• Timing and transition
• Impact and opportunities
Transition Commentary

“I continue to question whether all material weaknesses are being properly identified. It is surprisingly rare to see management identify a material weakness in the absence of a material misstatement.”

– Brian T. Croteau, Deputy Chief Accountant
  Office of the Chief Accountant
  U.S. Securities and Exchange Commission
“Unfortunately, over the decades, we’ve seen multiple cycles in which company management and internal and external auditors simply didn’t get it right in the area of internal control, resulting in failures to effectively define, understand, implement, and assess internal control.”

– Jeanette M. Franzel, Board Member
PCAOB
March 26, 2014
COSO is a joint initiative of five supporting organizations

1992 Original Framework

• Established a common internal control model against which companies and organizations may assess their control systems

Enhancing the Original Framework

• Updates to reflect changes in the business world over the past 20 years
Why update the original framework?

Original Framework

Refresh Objectives

Enhancements

Updated Framework


- Reflect changes in business & operating environments
- Expand focus on operations, compliance and non-financial reporting objectives
- Articulate principles to facilitate the development and assessment of internal control

- Updated, clarified and enhanced framework
- Broadens application: internal and non-financial reporting
- Clarifies requirements: Principles & Points of Focus


7
The Definition of Internal Control

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.
What is Remaining the Same?

- The three categories of objectives
- The five components of internal control
- The requirement to consider each of the five components to assess effectiveness
- The use of judgment in designing, implementing and evaluating the effectiveness of systems of internal control
What are the Key Changes?

Principles-based approach

- 5 components of internal control
- 17 principles that must be present and functioning in an effective system of internal control
- 81 points of focus are typically important characteristics of the 17 principles
What are the Key Changes?

17 principles are aligned with each of the five components

Requirements of COSO principles

• Must be present and functioning
• Must operate in an integrated manner

Added Points of Focus for each principle

• Important characteristics of principles
• Items management can consider to determine if the principles are present and functioning
# COSO Components & Principles

Update articulates 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 |
Points of Focus

Control Environment Component

Principle 1:
The organization demonstrates a commitment to integrity and ethical values

Points of focus:
- Sets the tone at the top
- Establishes standards of conduct
- Evaluates adherence to standards of conduct
- Addresses deviations in a timely manner

- Some points of focus may not be relevant
- Facilitate design, implementation, and assessment of internal control
- Not required to separately assess whether points of focus are in place
New Areas of Emphasis

**Governance**

- Enhanced focus on oversight role of the board of directors and its committees
- Board independence, skills and expertise
- Ensuring competence of personnel
- Board oversight of organization structure and reporting lines
- Appropriateness of communication with board
- Board responsibilities related to evaluating deficiencies and monitoring corrective actions
New Areas of Emphasis

Risk Assessment

- Increased focus on risk assessment process, and responding to assessed level of risk
- Importance of setting objectives
- Involvement of appropriate level of management
- Risk response evidenced by changes in control activities
- Risk assessment related to fraud (Principle 8)
- Assessment of changes to the external and internal business environment
New Areas of Emphasis

Information Technology

• 14 of the 17 principles include IT considerations
• Principle 11 focused on IT general controls
• Impact of system changes on internal control effectiveness
• Quality of data used to execute controls (Principle 13)
• Using relevant information
• Segregation of duties
• Use of data analytics – continuous monitoring
• Information security
New Areas of Emphasis

Outsourced Service Providers (OSPs)

- 12 of the 17 principles address monitoring of control activities performed by OSPs
- Management retains responsibilities for controls
- Inventory of OSPs with responsibilities related to key internal controls
- SOC1/SOC2 report evaluation
- Communication of integrity and ethical behavior requirements
- Competence and performance monitoring
- Accountability for internal control processes
Assessing the System of Internal Control

To conclude that your system of internal control is effective:

• The five components of internal control and all relevant principles must be:
  - Present and functioning
  - Operating together in an integrated manner

If a relevant principle is not present and functioning, a major deficiency exists in the system of internal control.
Timing and Transition

• Transition period:

• 2013 framework will supersede original framework at the end of the transition period

• During the transition period, entities reporting externally (and their auditors) should disclosure whether the original or updated version of the framework was used
Transition Commentary

“When SEC staff plans to monitor the transition for issuers using the 1992 framework to evaluate whether and if any staff or Commission actions become necessary or appropriate at some point in the future.”

– Paul Beswick, (Former) Chief Accountant
Office of the Chief Accountant
U.S. Securities and Exchange Commission
May 30, 2013
Next Steps

COSO has developed a plan to help guide the transition:

- **Step 1**: Develop awareness, expertise, and alignment
- **Step 2**: Conduct preliminary impact assessment
- **Step 3**: Facilitate broad awareness, training and comprehensive assessment
- **Step 4**: Develop and execute COSO transition plan for SOX compliance
- **Step 5**: Drive continuous improvement
Public Company Auditor Perspective

Auditors must evaluate whether the 17 principles are present and functioning by:

• Reviewing a map of a company’s existing internal controls over financial reporting to the 17 principles

• Evaluating any identified gaps

• Defining testing approach: Most likely to select controls impacting multiple principles and higher risk controls
Expect questions on focus areas:

- Risk Assessment
- IT
- OSPs

Auditors must evaluate deficiencies:

- Whether the 17 principles are present and functioning
- Whether deficiencies, in aggregate, indicate a material weakness exists
  - ELCs are generally indirectly related to financial statements and their evaluation is typically more qualitative that quantitative
Impact Will Vary by Organization

• Evaluate the 17 principles

• Map the existing internal controls to the 17 principles

• Evaluate whether each of the 17 principles and each of the five components are present and functioning, both individually and together, and document your findings

• Are there gaps? Does your system of internal control need to be updated to address all principles? Consider areas of emphasis

• Update internal control document
Lessons Learned

• Document relevant processes and controls that are not part of SOX
  - Management review items, data completeness and accuracy, commitment to competence
• Evaluate controls over OSPs/3rd party governance
• Focus only on key controls – ensure these are documented and monitored
• Consider mapping from key controls to COSO principles
• Get IA involved in the transition process – great perspective and will make it easier on you
• Auditor Facilitation – consider mapping to prior entity level controls
Risk of Not Remediating Gaps

SEC criteria for classifying internal control deficiencies:

• Material Weakness
• Significant Deficiency
• Control Deficiency

If a Material Weakness is present, management must conclude:

• Principle is NOT present and functioning
• System of Internal Control is NOT effective
Deficiency Assessment Examples

- Competence of Personnel
- Compensation Structure
- Vendor Management Program
- Data Quality
Principle Integration

Control Environment

Monitoring

Risk Assessment

Information & Communication

Control Activities

Internal Control System
Deficiency Assessment Examples

- Competence of Personnel
- Vendor Management Program
- Compensation Structure
- Data Quality
Principle Integration

Internal Control System

- Control Environment
- Risk Assessment
- Monitoring
- Information & Communication
- Control Activities
Deficiency Assessment Examples

- Competence of Personnel
- Compensation Structure
- Vendor Management Program
- Data Quality
Principle Integration

Internal Control System

- Control Environment
- Risk Assessment
- Monitoring
- Information & Communication
- Control Activities
Deficiency Assessment Examples

- Competence of Personnel
- Compensation Structure
- Vendor Management Program
- Data Quality
Principle Integration

Internal Control System

- Control Environment
- Risk Assessment
- Control Activities
- Information & Communication
- Monitoring
Other Opportunities

• Opportunity to refresh the internal control system and update controls documentation to evidence mapping

• Enhance controls around third-parties, IT systems, data security (including PII), and the quality and reliability of data

• Focus on all areas of reporting – including internal and non-financial reporting

• Update risk assessment processes, including fraud, as needed
Resources – New COSO Framework

COSO

• Internal Control – Integrated Framework Executive Summary
• Internal Control – Integrated Framework and Appendices
• Internal Control – Integrated Framework Internal Control over External Financial Reporting: A Compendium of Approaches and Examples
• Internal Control – Integrated Framework Illustrative Tools for Assessing Effectiveness of a System of Internal Control

AICPA

• The Updated COSO Framework
Questions?
Contact Information

Kim Mobley
kmoblej@johnsonlambert.com
678-534-5736

Jill Cleaveland
jcleaveland@johnsonlambert.com
678-534-2962

Greg Daniel
gdaniel@johnsonlambert.com
678-894-4273
Take Home Principle Detail
The organization demonstrates a commitment to integrity and ethical values.

**Points of Focus**

- Sets the tone at the top
- Establishes standards of conduct
- Evaluates adherence to standards of conduct
- Addresses deviations in a timely fashion
Principle 2

The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Points of Focus

- Establishes oversight responsibilities
- Applies relevant experience
- Operates independently
- Provides oversight on Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities
Principle 3

Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

Points of Focus

• Considers all structures of the entity
• Establishes reporting lines
• Defines, assigns, and limits authorities and responsibilities
Principle 4

The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

Points of Focus

- Establishes policies and practices
- Evaluates competence and addresses shortcomings
- Attracts, develops and retains individuals
- Plans and prepares for succession
Principle 5

The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Points of Focus

• Enforces accountability through structures, authorities and responsibilities
• Establishes performance measures, incentives and rewards
• Evaluates performance measures, incentives and rewards for ongoing relevance
• Considers excessive pressures
• Evaluates performance and rewards or disciplines individuals
Principle 6

The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives:

- Operational
- External Financial Reporting
- External Non-Financial Reporting
- Internal Reporting
- Compliance

Points of Focus

- Reflects management’s choices
- Considers tolerances for risk
- Includes operations and financial performance goals
- Forms a basis for committing of resources
- Complies with applicable accounting standards
- Considers materiality
- Reflects entity activities
- Complies with externally established standards and frameworks
- Considers the required level of precision
- Reflects external laws and regulations
Principle 7

The organization identifies risks to the achievement of its objectives across entity and analyzes risk as a basis for determining how the risks should be managed.

Points of Focus

- Includes entity, subsidiary, division, operating unit, and functional levels
- Analyzes internal and external factors
- Involves appropriate levels of management
- Estimates significance of risks identified
- Determines how to respond to risks
Principle 8

The organization considers the potential for fraud in assessing risks to the achievement of objectives.

Points of Focus

• Considers various types of fraud
• Assesses incentives and pressures
• Assesses opportunities
• Assesses attitudes and rationalizations
Principle 9

The organization identifies and assesses changes that could significantly impact the system of internal controls.

Points of Focus

- Assesses changes in the external environment
- Assesses changes in the business model
- Assesses changes in leadership
Principle 10

The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Points of Focus

- Integrates with risk assessment
- Considers entity-specific factors
- Determines relevant business processes
- Evaluates a mix of control activity types
- Considers at what level activities are applied
- Addresses segregation of duties
Principle 11

The organization selects and develops general control activities over technology to support the achievement of objectives.

Points of Focus

• Determines dependency between the use of technology in business processes and technology general controls
• Establishes relevant technology infrastructure control activities
• Establishes relevant security management process control activities
• Establishes relevant technology acquisition, development, and maintenance process control activities
The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

**Points of Focus**
- Establishes policies and procedures to support deployment of management’s directives
- Establishes responsibility and accountability for executing policies and procedures
- Performs in a timely manner
- Takes corrective action
- Performs using competent personnel
- Reassesses policies and procedures
Principle 13

The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

Points of Focus

• Identifies information requirements
• Captures internal and external sources of data
• Processes relevant data into information
• Maintains quality throughout processing
• Considers costs and benefits
Principle 14

The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

Points of Focus

- Communicates internal control information
- Communicates with the Board of Directors
- Provides separate communication lines
- Selects relevant method of communication
Principle 15

The organization communicates with external parties regarding matters affecting the functioning of internal control.

Points of Focus

• Communicates to external parties
• Enables inbound communication
• Communicates with the Board of Directors
• Provides separate communication lines
Principle 16

The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

Points of Focus

- Considers a mix of ongoing and separate evaluations
- Considers rate of change
- Establishes baseline understanding
- Uses knowledgeable personnel
- Integrates with business processes
- Adjusts scope and frequency
- Objectively evaluates
Principle 17

The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the Board of Directors, as appropriate.

Points of Focus

- Assesses results
- Communicates deficiencies
- Monitors corrective actions