Key Agenda Items

- Project Overview
- Summary of Updates
- Timeline for Implementation
- Codification of the Framework Principles
- Considerations and Implementation Steps
Project Overview
COSO Project Background

- In November 2010, COSO announced a project to **review and update** the “Internal Control – Integrated Framework” (Framework) originally issued in 1992.

- The decision to revise the original Framework was driven by the following factors:
  - The COSO Board’s desire to make the Framework more relevant and useful.
  - Business and operating environments have become more complex, technologically driven, and global in scale since the original Framework was issued more than 20 years ago.
  - Key stakeholders are more engaged and are seeking greater transparency and accountability for the integrity of “systems of internal control” that support business and governance.

- The Board of Directors of COSO approved the updated Framework and issued it on Tuesday, May 14, 2013. It incorporates input from various organizations (including the AICPA, IIA, public accounting firms, and regulators) and nearly 1,000 key stakeholders. The majority of respondents supported updating, but not overhauling the Framework.

- The revised Framework is expected to help organizations reduce risk, improve compliance, and strengthen internal controls.
Project Participants

The COSO Board engaged PwC to assist with the update, with input from an advisory council and various key stakeholders:

- **COSO Advisory Council**
  - AICPA
  - AAA
  - FEI
  - IIA
  - IMA
  - Public Accounting Firms
  - Regulatory observers
  - Others (IFAC, ISACA, others)

- **Stakeholders**
  - Over 700 stakeholders in original Framework responded to global survey during 2011
  - Over 200 stakeholders commented on proposed updates to original Framework during first quarter of 2012
  - Additional public exposure of proposed publications during fourth quarter of 2012
Integrated Framework: Overview

- First published in 1992
- Gained wide acceptance following the financial control failures in the early 2000s and initial SOX years
- Most widely used framework for evaluating controls in the U.S.
- Widely used around the world
- Most companies publicly disclose if they are following the Framework
Integrated Framework: Project Objectives

**Original Framework**

**Enhancement Objectives**

**Key Changes**

**Updated Framework**


- Address Significant Changes to the Business Environment and Associated Risks
- Codify Criteria Used in the Development and Assessment of Internal Control
- Increase Focus on Operations, Compliance, and Nonfinancial Reporting Objectives


- Updated, Enhanced, and Clarified Framework
- 17 Principles Aligned With the Five Components of Internal Control
- Expanded Internal and Nonfinancial Reporting Guidance
Summary of Updates
Integrated Framework: Key Changes

What Is Being Retained?

- The core definition of internal control.
- The three objectives of internal control.
- The five components of internal control.
- The requirement of five components for an “effective” system of internal control.
- The important role of “judgment” in designing, implementing, and conducting internal controls, and in assessing the effectiveness of internal controls.

What Is Changing?

- The addition of 17 principles underlying the original five components of internal control.
- Considerations related to changes in business, operating, and regulatory environments.
- Expanded financial reporting objectives to include other important forms of reporting.
- Additional approaches and examples relevant to operations, compliance, and nonfinancial reporting objectives.
Timeline for Implementation
Timeline for Implementation

- The updated Framework will supersede the original Framework.
- The original framework will remain available and appropriate for use through December 15, 2014, giving companies plenty of time to transition.
  - **Recommended Transition Period = January 1, 2014 through December 15, 2014**
- The issuance includes a volume titled “Illustrative Tools for Assessing Effectiveness of a System of Internal Control.” COSO also issued “Internal Control Over External Financial Reporting: A Compendium of Approaches and Examples,” which has been developed to assist users when applying the Framework to external financial reporting objectives.
- Users who are required to report upon the effectiveness of internal control should monitor guidance by regulators and standard-setters for any preference about which Framework to use for reporting purposes during the transition period.
- COSO believes continued use of the original Framework during the transition period would be acceptable.
- The SEC and PCAOB have not issued any formal transition or implementation guidance.
Codification of the Framework Principles
Core Definition of Internal Control

Effective internal controls are:

- Geared toward the achievement of three “objectives”:
  - Effectiveness and efficiency of operations
  - Reliability of reporting
  - Compliance with applicable laws and regulations
- A process: recurring tasks, activities, and policies and procedures
- Effected by people: actions taken at every level within an organization
- Able to provide reasonable assurance: not absolute assurance
- Adaptable to the entity’s structure: flexible in application
- Comprised of the five “components” of internal control working in an integrated manner:
  - Control environment
  - Risk assessment
  - Control activities
  - Information and communication
  - Monitoring activities
Requirements for “Effective Internal Control”

- The Framework “does not” prescribe requirements of specific controls that must be selected, developed, and deployed for an effective system of internal control. That determination is a function of “management judgment” based on factors unique to each entity, such as:
  - Laws, rules, regulations, and standards to which the entity is subject
  - Nature of the entity’s business and the markets in which it operates
  - Scope and nature of the management operating model
  - Competency of the personnel responsible for internal control
  - The entity’s use and dependence on technology
  - Management’s response to assessed risks
The phrase “present and functioning” is applied to components and principles:
- “Present” refers to the determination that components and relevant principles exist in the design of the system of internal control.
- “Functioning” refers to the determination that components and relevant principles continue to exist in the operation and conduct of the system of internal control.

A component or relevant principle that is present and functioning implies that the organization:
- Understands the intent of components and how relevant principles are being applied
- Helps personnel understand and apply relevant principles across the entity
- Views weakness in, or absence of a principle, as a situation that triggers management attention
Requirements for “Effective Internal Control” (continued)

- Senior Management and the Board of Directors must use judgment to assess whether each of the five components and relevant principles are present, functioning, and operating together in an integrated manner.

- When a component or relevant principle is deemed not present and functioning, or when components are deemed not operating in an integrated manner, a “major deficiency” exists. The PCAOB will need to determine if this classification will replace “significant deficiency” or “material weakness.”

- When a major deficiency exists, the entity cannot conclude that it has met the requirements for effective internal control.
### COSO’s Codification of Framework Principles

#### 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
7. Identifies and analyzes risk.
8. Assesses fraud risk.
9. Identifies and analyzes significant changes.

#### Control Activities
10. Selects and develops control activities.
11. Selects and develops general controls over technology.
12. Deploys through policies and procedures.

#### Information and Communication
13. Uses relevant information.
15. Communicates externally.

#### Monitoring Activities
16. Conducts ongoing and/or separate evaluations.
17. Evaluates and communicates deficiencies.

**Note**: Companies will need to link their internal controls to the 17 principles.
Integrated Framework: Enhancement Challenges

Enhancements that may cause significant challenges to management:

• **Risk Assessment**
  - Need for more detail discussions around risk concepts, inherent risk, and linkage between risk assessment and control activities
  - Consideration of fraud risk related to the assessment of risks for achievement of management objectives

• **Third-Party Outsourced Service Providers**
  - Framework asks for management to consider how outsourced service providers are monitored
  - Several references to service providers against many of the 17 principles

• **Information Technology (IT)**
  - Consideration of all uses of technology in the continuous monitoring process
  - Ensuring quality of information or data integrity
Principles and Attributes Related to the Control Environment Component

1. The organization demonstrates a commitment to integrity and ethical values.
   - Sets the tone at the top
   - Establishes standards of conduct
   - Evaluates adherence to standards of conduct
   - Addresses deviations in a timely manner
   - **KEY Example:** Evaluating Unethical and Fraudulent Behavior through independent hotline.

2. The Board of Directors demonstrates independence of management and exercises oversight for the development and performance of internal control.
   - Establishes Board of Directors oversight responsibilities
   - Retains or delegates oversight responsibilities
   - Operates independently
   - Provides oversight

3. Management establishes, with Board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
   - Considers all structures of the entity
   - Establishes reporting lines
   - Defines, assigns, and limits authorities and responsibilities
Principles and Attributes Related to the Control Environment Component (continued)

4. The organization demonstrates a commitment to attract, develop, and retain competent individuals.
   - Establishes policies, procedures, and practices
   - Evaluates competence and addresses shortcomings
   - Plans and prepares for succession

5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
   - Enforces accountability through structures, authorities, and responsibilities
   - Establishes performance measures, incentives, and rewards
   - Evaluates performance measures, incentives, and rewards for ongoing relevance
   - Evaluates performance and rewards or disciplines individuals
Principles and Attributes Related to the Risk Assessment Component

6. The organization specifies with sufficient clarity to enable the identification and assessment of risks relating to objectives (the chart below depicts attributes applicable to each objective category).

**KEY: Revised Financial Reporting into 3 separate objectives**

<table>
<thead>
<tr>
<th>OPERATIONS</th>
<th>INTERNAL</th>
<th>EXTERNAL NON-FINANCIAL</th>
<th>EXTERNAL FINANCIAL</th>
<th>COMPLIANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Considers Tolerance for Risk/Required Level of Precision/Materiality</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>b. Complies with Externally Established Standards and Frameworks/Complies with Applicable Accounting Standards/Reflects External Laws and Regulations</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>c. Reflects Management’s Choices</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>d. Reflects Entity Activities</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>e. Includes Operations and Financial Performance Goals</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>f. Forms Basis for Committing of Resources</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Principles and Attributes Related to the Risk Assessment Component (continued)

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

**KEY** Identify, Analyze, Respond

- Involves appropriate levels of management (Identify)
  - Entity, subsidiary, division, operating unit, and functional levels (Identify)
- Analyzes internal and external factors (Analyze)
- Estimates significance of risks identified (Identify)
- Determines how to respond to risks (Respond)

- Other factors to consider:
  - Identify and incorporate inherent risk factors
  - Expand risk assessment to include risk tolerance factors
  - Consider velocity of risks (how quickly changing), along with likelihood and impact
  - Remember to include impact of outsourced service providers and other third parties deemed impactful to the business
8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.

- Considers the various ways that frauds can occur
  - **KEY:** Align various fraud scenarios to control activities, and consider gaps in control structure to prevent fraud
- Assesses incentives and pressures, opportunities, attitudes, and rationalizations
- **Reminder:** Outsourced service providers and impactful third-party vendors can influence and cause potential fraud

9. The organization identifies and analyzes changes that could significantly affect the system of internal control.

- Analyzes changes in the external environment, changes in the business model, and changes in leadership
- Changes in technology systems, cloud computing, third-party access and outsourcing
Principles and Attributes Related to the Control Activities Component

10. The organization selects and develops control activities that contribute to the mitigation of risks to acceptable levels.
   - Determines relevant business processes
   - Considers entity-specific factors
   - Evaluates a mix of control activities and types
   - Considers at what level activities are applied
   - Addresses segregation of duties
   - **KEY:** Use of documentation of process flow, control activity, risk and control matrices, assessment of detective versus preventive controls, and SOC reports for outsourced service providers

11. The organization selects and develops general control activities over technology to support the achievement of objectives.
   - Determines dependency between the use of technology in business processes and technology general controls
   - Establishes relevant technology infrastructure control activities
   - Establishes relevant security management control activities
   - Establishes relevant technology acquisition, development, and maintenance control activities
Principles and Attributes Related to the Control Activities Component (continued)

12. The organization deploys control activities as manifested in policies that establish what is expected and in relevant procedures to effect the policies.
   - Establishes policies and procedures to support deployment of management directives
   - Establishes responsibility and accountability for executing policies and procedures
   - Performs procedures using competent personnel
   - Performs procedures in a timely manner
   - Takes corrective action
   - Reassess policies and procedures on a consistent and periodic basis
Principles and Attributes Related to the Information and Communication Component

13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal controls.
   - Identifies information requirements
   - Captures internal and external sources of data
   - Processes relevant data into information
   - Maintains quality throughout processing
   - Considers costs and benefits
   - **KEY:** Focus on reliability and protection of data

14. The organization communicates information with internal parties, including objectives and responsibilities for internal control, necessary to support the functioning of other components of internal control.
   - Communicates internal control information with personnel and the Board of Directors
   - Provides separate communication lines and selects relevant methods of communication
Principles and Attributes Related to the Information and Communication Component

15. The organization communicates information with external parties about matters affecting the functioning of components of internal control.
   - Communicates to external parties and with the Board of Directors
   - Provides separate communication lines and selects relevant methods of communication
   - **KEY:** Establish formal and periodic communication channels with third party and outsourced service providers – set in policy and procedures

16. The organization selects, develops, and performs ongoing and/or separate evaluations to determine whether the components of internal control are present and functioning.
   - Considers a mix of ongoing and separate evaluations
     - Ongoing – closer to operations of controls, earliest detection, self-assessment
     - Separate – risk focused, independently performed, validate on-going monitoring
   - Establishes a baseline understanding
   - Considers the rate of change
   - Uses knowledgeable personnel
   - Integrates with business processes
   - Objectively evaluates
   - **KEY:** Use of technology or data analytics monitoring
Principles and Attributes Related to the Monitoring Activities Component

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

- Assesses results
- Communicates deficiencies to Senior Management
- Reports deficiencies to Senior Management and the Board of Directors
- Monitors corrective actions
Considerations and Implementation Steps
Considerations – SOX

- The overall attestation process is not expected to materially change; however, there has been no guidance from regulators.
  - **KEY:** SEC and PCAOB have not weighed in, but are expected to later in 2014
- The new principles are expected to clarify how to apply the Framework in designing, implementing, conducting, and assessing the effectiveness of internal control.
  - **KEY:** External Auditors are communicating that they expect companies to show how they align the 17 principles to their control structure
- The new Framework modifies the classification of internal controls into two tiers:
  - **Major Deficiency:** A deficiency, or combination of deficiencies, that is severe enough to adversely affect the likelihood an entity can achieve its objectives.
  - **Internal Control Deficiency:** A shortcoming in a relevant principle or component that has the potential to adversely affect the ability of the entity to achieve its objective.
  - **KEY:** The PCAOB will evaluate whether these new classifications will replace the “deficiency,” “significant deficiency,” and/or “material weakness” classifications.
Considerations – SOX

- To transition from the original Framework to the updated Framework, Senior Management will need to assess how the entity’s system of internal control applies the 17 principles associated with the five components of internal control.
- The Board of Directors should discuss with Senior Management its plan to adopt the updated Framework and oversee management's assessment of any implications of, and determination of appropriate actions for, applying the updated Framework.
  - **KEY:** Boards and Audit Committees are starting to get educated, and having discussions with management about approach.
Considerations – ERM

- The COSO Board believes that enterprise risk management is broader in scope than internal control.
- The Board continues to believe that internal control is an integral part of enterprise risk management and the issuance of the updated Framework is not intended to affect that relationship.
- The Board believes there may be differing regulatory and stakeholder expectations relating to enterprise risk management and internal control.
- Entities may not be required by statute, rules, or standard setters to apply the “Enterprise Risk Management – Integrated Framework”; however, management may choose to do so to enhance its ability to create and sustain value.
- We are seeing many companies looking to integrate in COSO risk assessment with ERM program – looking for alignment and leverage.
Considerations – Expanded Reporting

- The Framework has been enhanced by expanding the financial reporting category of objectives to include other important forms of reporting, such as nonfinancial and internal reporting.

- The Framework reflects considerations of many changes in the business, operating, and regulatory environments over the past several decades, including:
  - Expectations for governance oversight
  - Globalization of markets and operations
  - Changes and greater complexity in the business
  - Demands and complexities in laws, rules, regulations, and standards
  - Expectations for competencies and accountabilities
  - Use of, and reliance on, evolving technologies
  - Expectations relating to preventing and detecting fraud

- Boards and other stakeholders are asking for more reporting, and COSO may be seen as a way to revised reporting components and provide more
Considerations – Other Opportunities

- This revision of the Framework can provide an opportunity to refresh the internal control structure, as well as add value in operations and compliance areas.
- Enhance or add an anti-fraud approach to risk management and the internal control structure.
- Improve corporate governance with ties into expanded financial reporting of operational and compliance areas.
- Greater focus and leverage of technology systems and controls, and third-party risks and controls.
- Opportunity to simplify key controls and gain leverage across greater upstream preventive controls, and compensating controls, leveraging the 17 principles.
- May identify gaps that existed before the revised Framework, thus adding additional assurance and control.
- Use of new and innovative evolving technologies in Governance, Risk, and Compliance (GRC) space.
Key Steps Towards Compliance

1. **Organize the Effort:** Educate the Board of Directors and Executive Management, establish a project team, and develop a project plan.

2. **Assess Existing Control Systems and Control Documentation:** Conduct an analysis of existing control systems related to reporting, operations and compliance (including a review of existing SOX and related regulatory documentation). Determine whether the five components and 17 principles are sufficiently documented and operating, and report gaps.

3. **Make Enhancements:** Enhance existing control systems or controls documentation. This may include controls systems encompassing reporting, compliance and operating objectives.
Key Steps – Organize the Effort

- Understand the Effort
  - The COSO Framework has been published in three volumes:
    1. “Internal Control – Integrated Framework: Executive Summary”: A high-level overview intended for the Board of Directors, Chief Executive Officer, other Senior Management, regulators, and standard setters.
    2. Framework and Appendices: Sets out the Framework, including the definition of internal control and the components and principles supporting effective systems of internal control.
    3. “Illustrative Tools for Assessing Effectiveness of a System of Internal Control”: Provides templates and scenarios that may be useful in applying the Framework.
  - In addition, “Internal Control Over External Financial Reporting: Compendium of Approaches and Examples” has been published to provide practical approaches and examples that illustrate how the components and principles set forth in the Framework can be applied in preparing external financial statements.
Key Steps – Organize the Effort

- Educate the Board of Directors and Executive Management
  - Provider overview of framework and changes
  - Seek input and information from external auditors
  - Discuss timing, impact, and effort, include any technology leverage as well

- Establish a project team
  - Cross-functional team
  - Internal Audit, Financial Owners (i.e., Controller, Compliance, etc.), key process owners
  - External Auditor as guest to provide observations and feedback, deemed necessary

- Develop a project plan
  - Step-by-step approach to implementation – timing, resource involvement
  - Consider educational or training needs of team, as well as process owners/employees
  - Build in efficiencies through use of technology tools or gap assessment avenues
Key Steps – Assessment of Controls

1. Assess Control Structure
   1. Conduct an analysis of existing controls related to reporting, operations and compliance
   2. Develop considerations – potential impact, fraud assessment, IT, other risk considerations
   3. Determine if there are certain areas/principles of Framework that are more concerning to your organization

2. Mapping Assessment Of Controls
   1. Map existing controls to 5 components and 17 principles to see if they are sufficiently documented and operating
   2. Perform review and evaluation to determine where existing controls do not align to Framework principles

3. Identify Gaps & Improvement Opportunities
   1. Based upon assessment, look for value add enhancements to controls to meet revised Framework
   2. Identify and document gaps by new controls, revisions, and replacements
   3. Review for documentation and test procedure changes

4. Remediation & Next Steps
   1. Development remediation plan with timing, key steps, and prioritization
   2. Report to Board and Management of revised effort and timing
   3. Perform remediation

5. Pilot and Communication
   1. Pick one key process area to walkthrough and test remediation efforts for effectiveness, before required implementation date
   2. Communicate Pilot and overall results to Board and Management
   3. Recommend process operational and compliance improvements to the Board
Today’s Presenters:

E. Michael Thomas  
Partner  
Crowe Horwath LLP  
3399 Peachtree Road, N.E., Suite 700  
Atlanta, GA 30326-2832  
Direct: 404-442-1607  
Fax: 404-442-1616  
Cell: 404-550-3492  
mike.thomas@crowehorwath.com

Sonny MacArthur  
Partner, Assurance & Advisory Services  
Porter Keadle Moore, LLC  
235 Peachtree Street, NE, Suite 1800  
Atlanta, GA 30303  
Direct: 404-420-5631  
Fax: 404-588-4222  
Cell: 404-931-7752  
smacarthur@pkm.com

Eric E. Bosch  
Director  
LaPorte, CPAs and Business Advisors  
111 Veterans Memorial Boulevard, Suite 600  
Metairie, LA 70005  
Direct: 504-838-4861  
Fax: 504-835-5535  
Cell: 504-908-1997  
ebosch@laporte.com

Questions??