2013 COSO Internal Control Framework Update

September 5, 2013
# Agenda – 2013 COSO IC Framework

<table>
<thead>
<tr>
<th>Topic</th>
<th>Minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>The update process</td>
<td>5</td>
</tr>
<tr>
<td>What is not changing / What is changing</td>
<td>5</td>
</tr>
<tr>
<td>The 17 principles and changes to the five components</td>
<td>30</td>
</tr>
<tr>
<td>Implementation and Next Steps</td>
<td>10</td>
</tr>
<tr>
<td>Q&amp;A</td>
<td>10</td>
</tr>
</tbody>
</table>
My current experience is with a:

A. Public company with ICFR audit requirement
B. Public company without ICFR audit requirement
C. Private company with internal control reporting requirements (such as financial institutions)
D. Private company without internal control reporting requirements
E. Public accounting firm
F. Other
My level of awareness of the changes to the COSO Framework is:

A. I have read the newly released Framework and followed the exposure draft process
B. I have read an article or summary of the changes
C. This presentation is my first look at the changes
D. I don’t know what COSO is; I just need CPE
The update process
COSO Evolution – Internal Control Publications

- **1992**: Internal Control — Integrated Framework
  - Executive Summary
  - Framework
  - Reporting to External Parties
  - Addendum to "Reporting to External Parties"

- **2006**: Internal Control over Financial Reporting - Guidance for Smaller Public Companies
  - Volume I: Executive Summary

- **2009**: Internal Control — Integrated Framework
  - Guidance on Monitoring Internal Control Systems
  - Volume I: Guidance

- **2013**: Internal Control — Integrated Framework
  - Framework and Appendices

---

Trust earned.
FreedMaxick, CPAs, P.C.

An Independently Owned Member
McGladrey Alliance
Why update what works? – The Framework has become the most widely adopted control framework worldwide.

**Original Framework**

**Refresh Objectives**

**Enhancements**

**Updated Framework**


- Reflect changes in business & operating environments
- Expand operations and reporting objectives
- Articulate principles to facilitate effective internal control

- Updates Context
- Broadens Application
- Clarifies Requirements

Intended benefits of updated Framework

- Improve governance
- Expand use beyond financial reporting
- Improve quality of risk assessment
- Strengthen IT guidance
- Strengthen anti-fraud efforts
- Adapt controls to changing business needs
- Greater applicability for various business models

Slide Source: COSO IC-IF Outreach Deck_12 29 11
(http://www.ic.coso.org/pages/about-the-project.aspx)
What is **not** changing vs. What **is** changing
What is not changing

- Objective setting foundation
- Definition of internal control
- The five components of internal control
  1. Control Environment
  2. Risk Assessment
  3. Control Activities
  4. Information & Communication
  5. Monitoring Activities
What is not changing (continued)

- COSO’s Enterprise Risk Management – Integrated Framework
  - The two frameworks remain distinct
Why – COSO Update expected to increase ease of use and broaden application

<table>
<thead>
<tr>
<th>What is not changing...</th>
<th>What is changing...</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Core definition of internal control</td>
<td>• Principles-based: Fundamental concepts underlying five components articulated as principles</td>
</tr>
<tr>
<td>• Three categories of objectives and five components of internal control</td>
<td>• Increased guidance/ease of use: Additional approaches and examples relevant to operations, compliance, and non-financial reporting objectives added</td>
</tr>
<tr>
<td>• Each of the five components of internal control are required for effective internal control</td>
<td>• Changes in business and operating environments considered</td>
</tr>
<tr>
<td>• Important role of judgment in designing, implementing and conducting internal control, and in assessing its effectiveness</td>
<td>• Operations and reporting objectives expanded</td>
</tr>
</tbody>
</table>
Update considers changes in business and operating environments

**Environments changes...**

- Expectations for governance oversight
- Globalization of markets and operations
- Changes and greater complexity in 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

**...have driven Framework updates**

COSO Cube (2013 Edition)
What is changing – COSO Cube

- Broadening of focus from “Financial Reporting” to “Reporting” – including internal and non-financial measures

- Clarifying definition of “Monitoring” to “Monitoring Activities” –

- Aligns organization structure with ERM Framework
What is changing (continued)

- Addition of 17 principles that are necessary for effective internal control (Must be in place or proven why not relevant)
- Describes 81 Points of Focus that are typically important characteristics of the principles (Do not need to be proven)
- Significant documentation considerations in transition
- Other changes to components
Transition

- Updated Framework was issued May 14, 2013
- COSO will continue to make available the original framework during the transition period extending to December 15, 2014, after which time COSO will consider it as having been superseded
- Early adoption is permitted
- Updated Framework supersedes existing Framework and *Internal Control over Financial Reporting – Guidance for Smaller Public Companies*
- Note: COSO is not a standards setting or enforcement body, see the SEC…
Which types of entities will be impacted by the changes to the Framework?

A. SEC registrants  
B. Non-profit organizations  
C. Commercial entities  
D. Financial institutions  
E. All of the above  
F. A and D only
Does this only impact SEC registrants?

- No – it will impact all companies that use COSO
- SEC registrants (large market cap currently subject to SOX) will likely have most significant impact
  - Certification
    - Will need to explicitly state which framework is being used during the period of transition (i.e., 1992 Framework or 2013 Framework)
  - Update SOX Documentation
  - Small public companies likely to move slower
Will all companies be required document their consideration of all 81 points of focus to demonstrate effective internal control?
A. Yes
B. No
The 17 principles and changes to the five components
Effective internal control

- Effective internal control provides reasonable assurance regarding the achievement of objectives and requires that:
  - Each component and each relevant principle is present and functioning
  - The five components are operating together in an integrated manner
### Internal control 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     | 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 &       | 13. Uses relevant information  
Communication       | 14. Communicates internally  
15. Communicates externally |
| Monitoring Activities| 16. Conducts ongoing and/or separate evaluations  
17. Evaluates and communicates deficiencies |

---

Slide Source: COSO IC-IF Outreach Deck_12 29 11  
(http://www.ic.coso.org/pages/about-the-project.aspx)
Control environment

The set of standards, processes, and structures that provide the basis for carrying out internal control across the organization.

Newly defined principles

1. The organization demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence of management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
Update describes important characteristics of principles as Points of Focus - Example

Control Environment

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

• Points of focus may not be suitable or relevant, and others may be identified
• Points of focus may facilitate designing, implementing, and conducting internal control
• There is no requirement to separately assess whether points of focus are in place
Under the updated Framework, if an entity does not have a board of directors, it fails principle 2 and does not have effective internal control.

A. True
B. False
C. It depends
Control environment – changes

- Five principles outline what is commonly called the “tone at the top”
- Expanded discussion and consideration of governance roles and notion of risk oversight
- Includes considerations for internal control in complex business environments
  - Outsourced service providers
  - Business partners
  - External partners
Risk assessment

A dynamic and iterative process for identifying and assessing risk to the achievement of objectives.

Newly defined principles

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

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

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

9. The organization identifies and assesses changes that could significantly impact the system of internal control.
Risk assessment – changes

- Principle specifically focused on consideration of fraud
- Clarifying risk assessment includes
  - Risk identification
  - Risk analysis
  - Note: Include Risk response and you have integrated with and implemented ERM
- Expands discussion on management’s need to understand changes in internal and external factors
Control activities

The actions established through policies and procedures that help ensure that management’s directives to mitigate risks to the achievement of objectives are carried out.

Newly defined principles

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

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

12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.
Control activities – changes

- Broadening discussion of technology
- Expanded discussion of automated control activities and general controls over technology
- Clarifies that control activities are actions established by policies and procedures not the policies and procedures themselves
Information and communication relates to external financial reporting only.

A. True
B. False
Information and communication

Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is the means by which information is disseminated throughout the organization. External communication enables inbound communication and provides external information.

Newly defined principles

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

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

15. The organization communicates with external parties regarding matters affecting the functioning of internal control.
- Emphasizes importance of quality of information
- Expands on reliability and protection of information
- Reflects impacts of technology on speed, means, and quality of flow of information
- Emphasizes importance of communication outside the entity (such as third-party service providers)
Monitoring activities

Ongoing evaluations, separate evaluations, or some combination of the two used to ascertain whether each of the five components of internal control are present and functioning.

Newly defined principles

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

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.
Monitoring activities - changes

- Clarifies that monitoring activities apply to all components of the Framework, not only control activities
- Includes two main categories of monitoring activities
  - Ongoing evaluations
  - Separate evaluations
- Expands discussion of technology and external service providers
Appendix C of the Framework provides considerations for smaller entities and governments.

Key consideration factors are provided for:
- Segregation of duties
- Management override
- Board of directors
- Information technology
- Monitoring activities
Next steps – internally

- Identify the appropriate individuals in your organization to be involved in the transition
  - Personnel familiar with your IT environment
  - Third party vendors/outsourced service providers
  - Personnel involved in anti-fraud programs

- Map your existing controls to the new Framework

- Prepare a gap analysis for the principles and points of focus

- Develop a plan to remediate identified gaps
Next steps – with your auditor

- Present your organization’s plan to map to the new Framework and assess gaps to your external auditor
- Present results of your gap analysis and remediation plan to your external auditor
- Collaborate on the impacts of any control changes on the current year audit engagement as well as changes for the year of adoption
Resources

  

- COSO Resources
  - *Internal Control-Integrated Framework*
    - Executive summary
    - Framework and Appendices
    - Illustrative tools for assessing effectiveness of a system of internal control
  - *Internal Control over External Financial Reporting, a Compendium of Approaches and Examples*
    - [www.coso.org](http://www.coso.org)
Questions?

Please feel free to contact:

Larry Hessney, PCI QSA, CIA, CISA
Director, Consulting Services
Risk and Technology Advisory
585.721.1508
Larry.hessney@freedmaxick.com