2013 COSO Framework
Deloitte Training
## Agenda

<table>
<thead>
<tr>
<th>Module</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module 1</td>
<td>COSO Background</td>
</tr>
<tr>
<td>Module 2</td>
<td>Objectives of Internal Control</td>
</tr>
<tr>
<td>Module 3</td>
<td>Effective Internal Control</td>
</tr>
<tr>
<td>Module 4</td>
<td>Additional Considerations</td>
</tr>
<tr>
<td>Module 5</td>
<td>Control Environment</td>
</tr>
<tr>
<td>Module 6</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>Module 7</td>
<td>Control Activities</td>
</tr>
<tr>
<td>Module 8</td>
<td>Information and Communication</td>
</tr>
<tr>
<td>Module 9</td>
<td>Monitoring Activities</td>
</tr>
<tr>
<td>Module 10</td>
<td>Considerations and Next Steps</td>
</tr>
<tr>
<td>Module 11</td>
<td>Resources Available</td>
</tr>
</tbody>
</table>
Course Objective

• Provide an overview of COSO’s structure and mission
• Provide an overview of the COSO\(^1\) 2013 framework, including:
  – What was carried forward
  – Broad changes
  – Transition guidance
• Conduct practical implementation examples facilitated through directed questions and activities
• Plan the considerations and next steps during the transition period, using the available tools and resources

\(^1\) Committee of Sponsoring Organizations of the Treadway Commission
Module 1

COSO Background
Background
COSO’s structure and mission

• COSO is a joint initiative of five sponsoring organizations
  – American Accounting Association (AAA)
  – American Institute of Certified Public Accountants (AICPA)
  – Financial Executives International (FEI)
  – Institute of Management Accountants (IMA)
  – Institute of Internal Auditors (IIA)

COSO’s mission is...

“…to provide thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations.”

www.coso.org/aboutus.htm
Background
Enhancing COSO’s 1992 Framework

• Project initiated to address changes in the business and operating environments since the 1992 Internal Control-Integrated Framework (the “1992 Framework”) was published

• Directed and supervised by COSO’s Board of Directors (the “Board”) with input from the following:
  – Over 700 survey respondents
  – An Advisory Council comprised of representatives from:
    • Companies
    • Academia
    • Government agencies
    • The accounting profession
    • Nonprofit organizations
  – Responses to public exposure of documents
# Background

Enhancing COSO’s 1992 Framework

<table>
<thead>
<tr>
<th>The update project includes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Executive Summary</td>
</tr>
<tr>
<td>• Internal Control — Integrated Framework (2013 Framework)</td>
</tr>
<tr>
<td>• Illustrative Tools for Assessing Effectiveness of a System of Internal Control</td>
</tr>
<tr>
<td>• Internal Control over External Financial Reporting (ICEFR): A Compendium of Approaches and Examples</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other COSO documents:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Guidance on Monitoring Internal Control Systems</td>
</tr>
<tr>
<td>• Enterprise Risk Management — Integrated Framework</td>
</tr>
</tbody>
</table>
Background
COSO transition guidance

• Transition period: **May 14, 2013 – December 15, 2014**
  – COSO will consider the 1992 Framework superseded after December 15, 2014

• If applying and referencing COSO’s Internal Control — Integrated Framework for external reporting purposes
  – External reporting should clearly disclose whether the 1992 or 2013 Framework was utilized
Transition
SEC and PCAOB

• The SEC has not issued formal transition guidance
  – SEC Chief Accountant Paul Beswick stated the following:
    • The “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. However, at this time, I’ll simply refer users of the COSO framework to the statements COSO has made about their new framework and their thoughts about transition.”

• The PCAOB has not issued formal or informal transition guidance to auditors
  – PCAOB Auditing Standard No. 5 requires the auditor to use the same internal control framework used by management
2013 Framework and guidance
What was carried forward from the 1992 Framework?

• 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 in the following categories:

• Effectiveness and efficiencies of operations
• Reliability of reporting
• Compliance with applicable laws and regulations”

• Five components of internal control

• Use of judgment in evaluating effectiveness of internal control
2013 Framework and guidance
General enhancements to the 1992 Framework

• The 2013 Framework:
  – Creates a more formal structure for the design and evaluation of the effectiveness of internal control
  – Adds and refreshes guidance within each of the components of internal control
2013 Framework and guidance
Structure

2013 Framework
- Components
- Principles
- Points of Focus

Illustrative Tools
- Templates
- Scenarios

ICEFR Compendium
- Approaches
- Examples
# 2013 Framework and Guidance

<table>
<thead>
<tr>
<th>Components</th>
<th>Summarized Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Environment</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>Risk Assessment</td>
<td>6. Specifies relevant 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>Control Activities</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>Information &amp; Communication</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>Monitoring Activities</td>
<td>16. Conducts ongoing and/or separate evaluations</td>
</tr>
<tr>
<td></td>
<td>17. Evaluates and communicates deficiencies</td>
</tr>
</tbody>
</table>
2013 Framework and Guidance

Specific significant enhancements to the 1992 Framework that may pose challenges to management:

Risk Assessment
- More detailed discussions about risk assessment concepts, including those related to inherent risk, risk tolerance, how risks may be managed, and linkage between risk assessment and control activities
- Considering the potential for fraud risk when assessing risks to the achievement of an organization’s objectives

Outsourced Service Providers (OSPs)
- Considerations related to OSPs are included throughout the framework, including 12 out of 17 principles
- Requires management to specifically consider how OSP’s are monitored

Information Technology (IT)
- Considerations related to IT are included in 14 of 17 principles
- Discussion of using IT to assist in continuous monitoring
- Requirements for ensuring quality of information (data integrity)
2013 Framework
Effective system of internal control

• Per COSO, an effective system of internal control requires:
  – Each of the five components of internal control and relevant principles to be present and functioning
  – The five components to be operating together in an integrated manner
Comparison of COSO to other rules
Effective system of internal control in ICEFR context

<table>
<thead>
<tr>
<th>COSO</th>
<th>SEC(^1)</th>
<th>PCAOB(^2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Present</strong>: the determination that components and relevant principles exist in the design and implementation of the system of internal control</td>
<td>• “Under the Commission’s rules, management’s annual assessment of the effectiveness of ICFR must be made in accordance with a suitable control framework’s [COSO] definition of effective internal control. These control frameworks define elements of internal control that are expected to be present and functioning in an effective internal control system.”</td>
<td>• <strong>Design effectiveness</strong>: Controls (if they are operated as prescribed by persons possessing the necessary authority and competence to perform the control effectively) that satisfy the company’s control objectives and can effectively prevent or detect errors or fraud that could result in material misstatements in the financial statements</td>
</tr>
<tr>
<td>• <strong>Functioning</strong>: the determination that components and relevant principles continue to exist in the conduct of the system of internal control</td>
<td></td>
<td>• <strong>Operating effectiveness</strong>: Controls that operate as designed and are performed by persons possessing the necessary authority and competence to perform the control effectively</td>
</tr>
</tbody>
</table>

---


\(^2\) As defined by Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 5, *An Audit of Internal Control Over Financial Reporting that is Integrated with an Audit of Financial Statements*; Para. 42–45
Comparison of COSO to other rules
Internal control deficiency in ICEFR context

<table>
<thead>
<tr>
<th>COSO</th>
<th>SEC&lt;sup&gt;1&lt;/sup&gt;</th>
<th>PCAOB&lt;sup&gt;2&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Internal control deficiency: A shortcoming in a component or components and relevant principle(s) that reduces the likelihood that the entity can achieve its objectives</td>
<td>• A deficiency in the design of ICFR exists when (a) necessary controls are missing or (b) existing controls are not properly designed so that, even if the control operates as designed, the financial reporting risks would not be addressed</td>
<td>• A deficiency in internal control over financial reporting exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis</td>
</tr>
</tbody>
</table>

<sup>1</sup> As defined by Securities Act Release No. 33-8810, File No. S7-24-06 (June 27, 2007); Footnote 29

<sup>2</sup> As defined by PCAOB Auditing Standard No. 5, An Audit of Internal Control Over Financial Reporting that is Integrated with an Audit of Financial Statements; Appendix A: Definitions, A3
## Comparison of COSO to other rules

### Significant deficiency in ICEFR context

<table>
<thead>
<tr>
<th><strong>COSO</strong></th>
<th><strong>SEC</strong></th>
<th><strong>PCAOB</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>COSO does not define <strong>significant deficiency</strong>, however, COSO acknowledges that when “an entity is applying a law, rule, regulation, or external standard, management should use only the relevant criteria contained in those documents to classify the severity of internal control deficiencies.”</td>
<td>The term <strong>significant deficiency</strong> means a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight of the registrant’s financial reporting.</td>
<td>A <strong>significant deficiency</strong> is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight of the company’s financial reporting.</td>
</tr>
</tbody>
</table>

---

1 As defined by Securities Act Release No. 33-8829, File No. S7-24-06 (September 10, 2007)

2 As defined by PCAOB Auditing Standard No. 5, *An Audit of Internal Control Over Financial Reporting that is Integrated with an Audit of Financial Statements*; Appendix A: Definitions, A11
Comparison of COSO to other rules
Major deficiency and material weakness in ICEFR context

<table>
<thead>
<tr>
<th>COSO</th>
<th>SEC(^1)</th>
<th>PCAOB(^2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• An internal control deficiency or combination of deficiencies that severely reduces the likelihood that the entity can achieve its objectives is referred to as a “<strong>major deficiency</strong>”</td>
<td>• The term <strong>material weakness</strong> is a deficiency, or a combination of deficiencies, in internal control over financial reporting such that there is a reasonable possibility that a material misstatement of the registrant’s annual or interim financial statements will not be prevented or detected on a timely basis</td>
<td>• A <strong>material weakness</strong> is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the company's annual or interim financial statements will not be prevented or detected on a timely basis</td>
</tr>
</tbody>
</table>

\(^1\) As defined by Securities Act Release No. 33-8809, File No. S7-24-06 (June 20, 2007)

\(^2\) As defined by PCAOB Auditing Standard No. 5, *An Audit of Internal Control Over Financial Reporting that is Integrated with an Audit of Financial Statements*; Appendix A: Definitions, A7
Module 2
Objectives of Internal Control
Relationship of Objectives, Components and the Entity

Definitions

- **Objectives**: Are what an entity desires to achieve.
- **Components**: Represent what is required to achieve objectives.
- **Entity Structure**: Represent the operating units, legal entities and other structures

A direct relationship exists between objectives, components, and the entity structure which can be depicted in the form of a cube.

- The objectives are represented by the columns.
- The components are represented by the rows.
- The entity structure is represented by the third dimension of the cube
Objectives Defined

“Internal control is a process effected by an entities board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance.”

Management, with board oversight, sets entity level objectives that align with the entity’s vision, mission & strategies. The framework groups objectives into the following three categories:

• Operations – Pertain to the effectiveness and efficiency of the entity’s operations, including operational and financial performance goals and safeguarding of assets against loss.

• Reporting – Pertain to internal and external financial and non financial reporting. Encompasses reliability, timeliness, transparency and other characteristics defined by regulators, standard setters or the entity’s policy.

• Compliance – Pertain to the adherence to laws and regulations to which the entity is subject.
Objectives - Operations

“Operations objectives relate to the achievement of an entity’s basic mission and vision – the fundamental reason for it’s existence.”

• These objectives relate to all entities but will vary based on management’s choices relating to operating model, industry considerations, and the entities performance.

• May relate to improving financial performance, productivity, quality, environmental practices, innovation, customer satisfaction etc.

• If an entity’s operations objectives are not well defined (i.e., aligned to mission & vision) or clearly specified its resources may be misdirected.
Objectives – Operations (cont.)

The operations objective includes safeguarding of assets
• Entities may set objectives relating to the prevention of loss of assets and the timely detection and reporting of any such losses
• These objectives form the basis of assessing risk relating to the safeguarding of assets and selecting and developing controls needed to mitigate such risk
• Some entities consider safeguarding of assets a separate category of objective

“Laws, rules, regulations, and external standards have created an expectation that management reporting on internal control includes controls relating to preventing and detecting unauthorized acquisition, use, or disposition of entity assets.”
Objectives – Reporting

Pertains to the preparation of reports for use by organizations and stakeholders and may relate to financial or non-financial reporting and to internal or external reporting.

- **External Financial Reporting Objectives**
  - Annual Financial Statements
  - Interim Financial Statements
  - Earning Releases

- **External Non-Financial Objectives**
  - Internal Control Reports
  - Sustainability Reports
  - Supply Chain / Custody of Assets

- **Internal Financial Reporting Objectives**
  - Divisional Financial Reports
  - Customer Profitability Analysis
  - Bank Covenant Calculations

- **Internal Non-Financial Objectives**
  - Staff / Asset Utilization
  - Customer Satisfaction Measures
  - Health and Safety Measures
Objectives – Compliance

The compliance objective pertains to the adherence to applicable laws and regulations that apply across the entity.

- As part of specifying compliance objectives, organizations need to understand which laws, rules and regulations apply across the entity.
- Laws, rules and regulations establish minimum standards of conduct expected of the entity. Entities are expected to incorporate these standards into the objectives set for the organization.
  - Some entities will set objectives utilizing a higher level of performance and management can exercise discretion in this regard
  - For example, while a law may limit minors working more than 18 hours in a school week, an organization may set an objective that limits its minor-age staff to working 15 hours per week.
Module 3
Effective Internal Control
Module 3 - Agenda

• Requirements for Effective Internal Control

• Suitability & Relevance of Components and Principles
  a) Present & Functioning
  b) Operating Together in an Integrated Manner

• Deficiencies in Internal Control
2013 Framework
Requirements for Effective Internal Control

• Per COSO, an effective system of internal control requires:
  – Achievement of objectives relating to one, two, or all three objective categories (i.e., operations, reporting, and compliance)
  – Each of the five components of internal control and relevant principles to be present and functioning
  – The five components and relevant principles to be operating together in an integrated manner

[Image of a diagram with the following components:
- Control Environment
- Risk Assessment
- Information and Communication
- Control Activities
- Monitoring]
COSO Internal Control Framework

Requirements for Effective Internal Control

For *internal control to be effective*, senior management and the board of directors have reasonable assurance of the following categories of objectives:

- Operations
- Reporting
- Compliance

For an effective system the senior management should have *reasonable assurance* that the system of internal control reduces to an acceptable level, the risk of not achieving an objective relating to one, two, or all three categories.
COSO Internal Control Framework
Suitability & Relevance of Components and Principles

• The Framework views all components of internal control as suitable and relevant to all entities.

• The 17 principles explain the concepts associated with the five COSO components. As such, the presumption is that all 17 principles are relevant to all entities.

• If a relevant principle is not present and functioning, the associated component cannot be present and functioning.
  – In the rare instance that Management determines that a principle is not relevant to a component, Management must support its determination that a principle is not relevant with the rationale of how, in the absence of that principle, the associated component can be present and functioning.

Note: While the points of focus may help management design, implement, and evaluate internal control and assess whether relevant principles are present and functioning, they are not required for assessing the effectiveness of internal control.
COSO Internal Control Framework
Suitability & Relevance of Components and Principles: Present & Functioning
Per 2013 Framework, an effective system of internal control requires each of the five components and relevant principles to be present and functioning.

• **Present** is defined as “the determination that components and relevant principles exist in the design and implementation of the system of internal control to achieve specified objectives.”

• **Functioning** is defined as “the determination that components and relevant principles continue to exist in the conduct of the system of internal control to achieve specified objectives.”
COSO Internal Control Framework

Suitability & Relevance of Components and Principles: Operating Together

*Operating together* refers to “the determination that all five components collectively reduce, to an acceptable level, the risk of not achieving an objective.”

Management can demonstrate that components operate together when:

- The “components are present and functioning.”
- “Internal control deficiencies aggregated across components do not result in the determination that one or more major deficiencies exist.”
# Key Terminology Updates - Overview

## Deficiency Terminology Comparison

<table>
<thead>
<tr>
<th>Deficiency</th>
<th>COSO</th>
<th>SEC</th>
<th>PCAOB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Control Deficiency</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deficiency</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Significant Deficiency</td>
<td>COSO does not define <strong>significant deficiency</strong>, although they do note, &quot;For purposes of applying the Framework to external financial reporting, management must apply laws, rules, regulations, and standards appropriate for the entity in evaluating, classifying, and reporting internal control deficiencies.&quot;</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Major Deficiency (equivalent of material weakness)</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Material Weakness (equivalent of major deficiency)</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Effective Internal Control
Operating together in an integrated manner

- The template below is an *Illustrative Tool* that can be used as a logical structure to help management analyze and document the organization's assessment of internal control, including the requirement that the five components and relevant principles operate together in an integrated manner.

- Once you have identified a control deficiency, how do you plan to assess the impact to other components?

<table>
<thead>
<tr>
<th>Overall Assessment of a System of Internal Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity or part of organization structure subject to the assessment (entity, division, operating unit, function)</td>
</tr>
<tr>
<td>Objective(s) being considered for the scope of internal control being assessed</td>
</tr>
<tr>
<td>Operations, Reporting, Compliance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Control Environment</th>
<th>Present? (Y/N)</th>
<th>Functioning? (Y/N)</th>
<th>Explanation/Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Assessment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control Activities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information and Communication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring Activities</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- *Are all components operating together in an integrated manner?*
  - Evaluate if a combination of internal control deficiencies, when aggregated across components, represent a major deficiency?
  - *(Update Summary of Deficiencies Template as needed)*

- *Is the overall system of internal control effective? (Y/No)*
  - Basis for conclusion

* If it is determined that there is a major deficiency, management must conclude that the system of internal control is not effective.
Activity: Evaluating Control Deficiencies

Refer to the *Illustrative Tool* in the previous slide to help you think of how to assess the effectiveness of the system of internal control and document the assessment to ensure the 5 components are operating together in an integrated manner in the examples below.

As a table group, discuss the following examples:

1. Errors were identified in a critical excel analysis supporting warranty reserves. The analysis included and incorrect formula. Further, due to recent significant quality issues, and an incorrect assumption was used. Both errors resulted in an understatement of the p&l and an under accrual in the warranty reserve. Errors were identified by the auditors.

2. A company had a significant FCPA violation related to payments being made to a government official in China. The company found out about the violation when one of their managers in China was arrested.

Which principles and components have been impacted by these deficiencies? Consider whether the principles are present and functioning and operating together in an integrated manner.

---

Read Handout – 5 minutes
Table Activity – 5 minutes
Group Debrief – 10 minutes
Module 4

Additional Considerations
Module 4 - Agenda

• Judgment
• Points of focus
• Controls to effect principles
• Organizational boundaries
• Technology
• Larger versus smaller entities
• Benefits and costs of internal control
• Documentation
Judgment

“An effective system of internal control demands more than rigorous adherence to policies and procedures: it requires the use of judgment.”

- Management exercises judgment in areas such as:
  - Applying internal control components relative to categories of objectives
  - Applying internal control components and principles within the entity structure
  - Specifying suitable objectives and sub-objectives and assessing risks to achieving these objectives
  - Selecting, developing, and deploying controls necessary to effect principles
  - Assessing whether components are present, functioning, and operating together
  - Assessing whether principles are relevant to the entity and present and functioning
  - Assessing the severity of internal control deficiencies
Points of focus

- Important characteristics of the principles – 87 in total
- Assist management in designing, implementing and evaluating internal control and assessing whether relevant principles are present and functioning
- May determine some are not suitable or relevant and others may be identified
- Framework does not require that management assess separately that the points of focus are in place when evaluating the effectiveness of internal control

**Control component:**

**Control environment**

**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
Controls to effect principles

- The Framework does not prescribe specific controls that must be selected, developed and deployed for an effective system of internal controls.
- The controls an organization selects to effect the principles and components is a function of management judgment based on factors unique to the organization.
- The absence of controls necessary to effect the relevant principles represents an internal control deficiency.
- Management may consider other controls (whether or not associated with that particular component or principle) that compensate for an internal control deficiency.

<table>
<thead>
<tr>
<th>Control component:</th>
<th>Control activities</th>
</tr>
</thead>
</table>

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

Controls embedded in other components may effect this principle, e.g.:

- Control Activity #1 Risk Assessment
- Control Activity #2 Information & Communication
- Control Activity #3 Monitoring Activities
Organizational boundaries

• One of the significant additions to the 2013 Framework is the incorporation of considerations related to outsourced service providers (OSPs.)
• In today’s environment, many organizations choose to outsource business or information technology processes and related activities to OSPs.
• Dependency on OSPs changes the risks of business activities, increases the importance of the quality of information and communications from outside the organization, and creates challenges in overseeing activities and related controls.
• Management still retains responsibility for the system of internal control.
• Important for users of the 2013 Framework to consider how the use of OSPs may effect the components and relevant principles within their overall system of internal control
• Third Party (i.e. vendors) vs. OSPs
Activity: Outsourced Service Providers

Refer to Handout 1 – Heads Up: COSO Enhances its Internal Control — Integrated Framework (6/10/13) – **Appendix B** - Summary of Concepts and Discussion in the 2013 Framework Related to the Use of Outsourced Service Providers (OSPs)

As a table group, discuss the following questions:

1. Have you identified a population/inventory of OSPs where key internal controls have been outsourced and evaluated the effectiveness of your Company’s monitoring procedures over the control activities performed by the OSPs? Do your contracts with OSP’s contain a requirement to provide a SOC1/SOC2 report?

2. How does the entity ensure the organization’s expectations for integrity and ethical values are understood by the OSP’s?

3. As companies may now need to enhance existing practices and documentation around third-party oversight/governance, do you think your company has solid controls around OSP’s?

**Read Handout** – 5 minutes

**Table Activity** – 5 minutes

**Group Debrief** – 10 minutes
Technology

• The Framework uses the term “technology” to refer to all computerized systems, including software applications running on a computer and operational control systems.
• The principles presented in the 2013 Framework do not change with the application of technology.
• Technology affects how an organization designs, implements, and conducts internal control; but, the same principles remain suitable and relevant.
Activity: Technology


As a table group, discuss the following questions:

1. How have you considered changes in IT and their impact on control effectiveness?
2. How do you leverage IT to support completeness and accuracy of information?
3. How do you leverage IT to support continuous monitoring?
4. Have you considered how effective your IT security system is, with respect to internal security and external security, i.e. cyber security?

Read Handout – 5 minutes
Table Activity – 5 minutes
Group Debrief – 10 minutes
Larger versus Smaller Entities

• Internal control components and principles are applicable for both large and small entities; however, implementation approaches may vary.

Benefits and costs of internal control

• Internal control provides many benefits to an entity; however, there are costs that Management must weigh to strike the right balance of making the right use of the entity’s resources, mitigating the areas of greatest risk and complexity and meeting the entity’s objectives.

Documentation

• Management must determine the level/extent of documentation needed to assess the effectiveness of internal control.
• Some level of documentation is always necessary to assure management that each of the components and relevant principles is present and functioning and components are operating together.
Module 5

Control Environment
Module 5 - Agenda

- Control Environment Overview
- Discussion of Principles
  - Points of Focus
  - Enhanced Aspects
  - ICEFR Approaches and Examples
Control Environment Overview

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

Principles of Component
Principle 1
Demonstrates Commitment to Integrity and Ethical Values

“The organization demonstrates a commitment to integrity and ethical values”

• Management and the board of directors or equivalent oversight body establish the standards and mechanisms for the organization to understand and adhere to doing what is right, and define the process and resources for interpreting and addressing the potential for deviations.

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
**Principle 1**
Demonstrates Commitment to Integrity and Ethical Values (cont.)

**Summary of Enhanced Concepts of Principle 1:**

- Integrity as a prerequisite to ethical behavior and an effective system of internal control
- Need to consider impacts of control environment across the structure
- Importance of:
  - Tone at the top as set by the board of directors and management
  - Establishing standards of conduct for employees and outsourced service providers (OSPs)
  - Evaluating adherence to expected standards and addressing any deviations in a timely manner
**Principle 1**  
Demonstrates Commitment to Integrity and Ethical Values (cont.)

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Establishing standards of conduct</td>
<td>• Defining, communicating, and regularly updating the code of business conduct and ethical standards</td>
</tr>
<tr>
<td>• Leading by example on matters of integrity and ethics</td>
<td>• Using a company newsletter to reinforce expectations of integrity and ethics</td>
</tr>
<tr>
<td>• Evaluating management and other personnel, outsourced service providers, and business partners for adherence to standards of conduct</td>
<td>• Evaluating misconduct reported through an anonymous hotline</td>
</tr>
<tr>
<td>• Developing processes to report and promptly act on deviations from standards of conduct</td>
<td>• Conducting Ethics Audits</td>
</tr>
<tr>
<td></td>
<td>• Taking action when deviations occur</td>
</tr>
</tbody>
</table>
ICEFR Compendium - Example
Evaluating Misconduct Reported through an Anonymous Hotline

All-World Food Distributors provides an anonymous hotline for employees to report potential fraud and other ethical concerns. The entity engages a third-party service provider to administer the hotline to provide the comfort of anonymity for its employees. This service immediately reports any potential illegal acts or financial reporting improprieties directly to the company’s legal department and audit committee. Issues and trends are analyzed and conclusions are reported to the audit committee of the board.
Discussion Question

As it relates to the whistle blower hotline, how would management demonstrate that the program is effective? What documentation/evidence of the program's effectiveness would support this?
Principle 2
Exercises Oversight Responsibility

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

- The board of directors or equivalent oversight body (the “board”) understands the business and expectations of stakeholders, including customers, employees, investors, and the general public, as well as legal regulatory requirements and related risks

Points of Focus
- Establishes oversight responsibilities
- Applies relevant expertise
- Operates independently
- Provides oversight for the system of internal control
## Principle 2
Exercises Oversight Responsibility (cont.)

<table>
<thead>
<tr>
<th>Summary of Enhanced Concepts of Principle 2:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Expanded discussion of governance concepts, including the need to establish oversight responsibilities for the board and its committees</td>
</tr>
<tr>
<td>• Matters related to board independence, skills, and expertise</td>
</tr>
<tr>
<td>• Includes a detailed table illustrating board oversight responsibilities for each of the five components of internal control</td>
</tr>
</tbody>
</table>
## Principle 2
### Exercises Oversight Responsibility (cont.)

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Establishing the roles, responsibilities, and delegation of authority of the board of directors</td>
<td>• Reviewing and documenting key activities of the audit committee</td>
</tr>
<tr>
<td>• Establishing policies and practices for meetings between the board of directors and management</td>
<td>• Establishing an audit committee meeting calendar</td>
</tr>
<tr>
<td>• Identifying and reviewing board of director candidates</td>
<td>• Changing the board composition of a closely held company</td>
</tr>
<tr>
<td>• Reviewing management’s assertions and judgments</td>
<td>• Assessing and Disclosing Director Qualifications</td>
</tr>
<tr>
<td>• Obtaining an external view</td>
<td>• Reviewing financial statement estimates</td>
</tr>
<tr>
<td>• Considering whistle-blower information about financial statement errors and irregularities</td>
<td>• Interacting with auditors</td>
</tr>
<tr>
<td></td>
<td>• Assessing the potential of management override</td>
</tr>
<tr>
<td></td>
<td>• Investigating and reporting whistle-blower allegations</td>
</tr>
</tbody>
</table>
ICEFR Compendium - Example
Reviewing and documenting key activities of the audit committee

Every year the board of Directors of Northern Power, a distributor of electricity, commissions an effective evaluation of its audit committee. An independent consultant with expertise in governance reviews the means by which the audit committee fulfills its responsibilities, as set out in its charter. Specially, it evaluates how the member of the audit committee:

- Oversee the quality and reliability of financial reporting and disclosures
- Understand the key risks facing the organization and the processes management uses to identify, assess and manage risks, considering internal audit findings, litigations, compensation schemes, regulations and compliance
- Evaluate organizational behavior, culture, and adherence to standards of conduct
- Challenge management and the external auditor in determining materiality for financial reporting purposes
- Assess reasonableness and appropriateness of critical accounting policies of the company
- Confirm or reject the basis for management estimates and proposed accounting policies changes before approving
- Evaluate, retain, or change external auditors
- Review audit plans
- Review management’s assessment of internal control over external financial reporting

The results of the evaluation are used to determine whether the roles and responsibilities of the committee have been met and could result in committee member changes or impact remuneration. In addition to the annual review, every three years the company conducts a benchmark review against leading practices and refines its charter as appropriate.
**Principle 3**  
**Establishes Structure, Authority, and Responsibility**

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

- Senior management and the board of directors establish the organizational structure and reporting lines necessary to plan, execute, control, and periodically assess the activities of the entity, in other words carry out their oversight responsibility

---

**Points of Focus**

- Considers all structures of the entity
- Establishes reporting lines
- Defines, assigns, and limits authorities and responsibilities
  - Board of Directors
  - Senior Management
  - Management
  - Personnel
  - Outsourced Service Providers
**Principle 3**  
Establishes Structure, Authority, and Responsibility (cont.)

<table>
<thead>
<tr>
<th>Summary of Enhanced Concepts of Principle 3:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Defining, assigning, and limiting authority and responsibility at different organizational levels and along the various lines of reporting (e.g., considering product or service lines, legal entity structures, geographical markets, and arrangements with OSPs).</td>
</tr>
</tbody>
</table>
### Principle 3
Establishes Structure, Authority, and Responsibility (cont.)

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Defining roles and reporting lines and assessing them for relevance</td>
<td>• Reorganizing to support control structure</td>
</tr>
<tr>
<td>• Defining authority at different levels of management</td>
<td>• Redefining roles with CEO and Board input</td>
</tr>
<tr>
<td>• Maintaining job descriptions and service-level agreements</td>
<td>• Maintaining an authority and approval matrix</td>
</tr>
<tr>
<td>• Defining the role of internal auditors</td>
<td>• Aligning roles and responsibilities with objectives</td>
</tr>
<tr>
<td></td>
<td>• Maintaining control while engaging outside service providers</td>
</tr>
<tr>
<td></td>
<td>• Reviewing and approving the internal audit plan</td>
</tr>
</tbody>
</table>
ICEFR Compendium - Approach
Defining authority at different levels of management

• The board of directors outlines its oversight authority for financial reporting over senior management through its charter. When assigning authorities and responsibilities, management considers the impact on the control environment and the importance of effectively segregating duties. Policy documents define cascading levels of authority, checks, and balances for authorizing transactions, and accounting and reporting of financial results. Such authority and responsibility is deliberately limited in order to balance the need for the efficient achievement of objectives against the risks that could result from unmonitored inappropriate conduct. Management empowers employees to correct problems or implement improvements in their assigned business process as necessary.
Principle 4
Demonstrates Commitment to Competence

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

• Policies and practices provide the foundation for defining the competence needed within the organization and provide the basis for more detailed procedures for executing and evaluating performance as well as determining remedial actions, as necessary

<table>
<thead>
<tr>
<th>Points of Focus</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Establishes policies and practices</td>
</tr>
<tr>
<td>• Evaluates competence and addresses shortcomings</td>
</tr>
<tr>
<td>• Attracts, develops, and retains individuals</td>
</tr>
<tr>
<td>• Plans and prepares for succession</td>
</tr>
</tbody>
</table>
**Summary of Enhanced Concepts of Principle 4:**

- Planning and preparing for succession for those roles that are important to the effectiveness of internal control
- Expectation and evaluation of competencies
- Incorporates consideration of OSPs
## Principle 4
Demonstrates Commitment to Competence (cont.)

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Establishing required knowledge, skills, and expertise</td>
<td>• Periodically reviewing policies</td>
</tr>
<tr>
<td>• Linking competence standards to established policies and practices in hiring, training, and retention decisions</td>
<td>• Recruiting and retaining key financial reporting positions</td>
</tr>
<tr>
<td>• Identifying and delivering financial reporting-related training as needed</td>
<td>• Defining performance expectations</td>
</tr>
<tr>
<td>• Selecting appropriate outsourced service providers</td>
<td>• Implementing complex accounting standards</td>
</tr>
<tr>
<td></td>
<td>• Retaining external tax assistance</td>
</tr>
</tbody>
</table>
**Principle 4**  
**Demonstrates Commitment to Competence (cont.)**

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Evaluating competence and behavior</td>
<td>• Periodically assessing performance</td>
</tr>
<tr>
<td>• Evaluating the capacity of finance personnel</td>
<td>• Audit Committee review of manager roles</td>
</tr>
<tr>
<td>• Developing alternate candidates for key finance reporting roles</td>
<td>• Assessing the adequacy of staffing levels for financial reporting</td>
</tr>
<tr>
<td></td>
<td>• Aligning competencies with key financial reporting positions</td>
</tr>
<tr>
<td></td>
<td>• Addressing succession planning</td>
</tr>
</tbody>
</table>
ICEFR Compendium - Example
Assessing the Adequacy of Staffing Levels for Financial Reporting

• The senior management of Tall Tree Finance, an investment bank and institutional securities company, annually assesses the adequacy of staffing levels of its key financial reporting function to understand and manage effectively the company’s current business activities, related accounting questions, and IT implementation challenges. The audit committee oversees this assessment.

• In particular, the assessment considers how adequately personnel respond to emerging accounting, reporting, and internal control issues. Senior management uses the results of this assessment to make decisions on staff training, reassignments, or other organizational changes.
Principle 5
Enforces Accountability

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

- The board of directors ultimately holds the chief executive officer accountable for understanding the risks faced by the entity and establishing the requisite system of internal control to support the achievement of the entity’s 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 5
Enforces Accountability (cont.)

### Summary of Enhanced Concepts of Principle 5:

- The importance of holding individuals accountable for their internal control responsibilities
- Aligning incentives and rewards with internal control responsibilities
- Considering excessive pressures
- Incorporates consideration of OSPs
**Principle 5**
Enforces Accountability (cont.)

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Defining and confirming responsibilities</td>
<td>• Cascading responsibilities throughout the organization and certifying results</td>
</tr>
<tr>
<td>• Developing balanced performance measures, incentives, and rewards</td>
<td>• Defining and communicating the basis for reward</td>
</tr>
<tr>
<td>• Evaluating performance measures for intended influence</td>
<td>• Establishing and overseeing performance measures, incentives, and rewards</td>
</tr>
<tr>
<td>• Linking compensation and other rewards to performance</td>
<td>• Aligning incentives with ethics and values</td>
</tr>
<tr>
<td></td>
<td>• Providing recognition for suggestions made to enhance internal control</td>
</tr>
</tbody>
</table>
Modern Financial Services has implemented a rewards system that requires the achievement of defined performance measures and encourages departments to monitor the effectiveness of their internal control systems and to self-report possible control deficiencies or opportunities for enhancement. This encouragement comes in the form of a policy that gives departments credit in the internal audit grading system for self-reported deficiencies. Any deficiencies that are identified through internal audit procedures, rather than through a department’s monitoring efforts, are counted against the score.

The credit does not preclude the internal audit department from reporting specific deficiencies to management or the board when warranted, but it does positively affect the grading system, which can affect departmental compensation and benefits. The result is that Modern Financial Services is more likely to identify control deficiencies before they can become material to the organization.
Activity: Identify Component Controls

- Refer to Handout 2, which is the summary of Components, Principles and Points of Focus.
- Identify relevant controls that address the principles within the assigned component. Consider the points of focus to assist in the identification of relevant control activities.
- Flipchart the:
  - Relevant controls identified for each principle
  - Control gaps identified for each principle

Prepare Responses – 15 minutes
Debrief Responses – 10 minutes
Activity #1 – Flipchart Example

COMPONENT: Control Environment

<table>
<thead>
<tr>
<th>Control</th>
<th>Principle#1</th>
<th>Principle#2</th>
<th>Principle#3</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA#1</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CA#2</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>CA#3</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>n/a</td>
<td></td>
<td>GAP</td>
<td></td>
</tr>
</tbody>
</table>
Module 6
Risk Assessment
Module 6 - Agenda

• Risk Assessment Overview

• Discussion of Principles
  – Points of Focus
  – Enhanced Aspects
  – ICEFR Approaches and Examples
Risk Assessment Overview

Principles of Component

6. Specify Suitable Objectives
7. Identify and Analyze Risks
8. Assess Fraud Risk
9. Identify and Analyze Significant Change
Principle 6
Specifies Suitable Objectives (cont.)

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

- Principle 6 is organized into three distinct sections, each with different points of focus:

<table>
<thead>
<tr>
<th>Points of Focus:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Operations Objectives</td>
</tr>
<tr>
<td>• Reporting Objectives</td>
</tr>
</tbody>
</table>
  - External Financial Reporting Objectives
  - External Non-financial Reporting Objectives
  - Internal Reporting Objectives
| • Compliance Objectives |

- **Enhanced Aspects of Principle 6:** Separates the financial reporting category into three separate objectives
**Principle 6**
Specifies Suitable Objectives (cont.)

**Operations Objectives**

**Points of Focus**
- Reflects management’s choices
- Considers tolerance for risk
- Includes operations and financial performance goals
- Forms a basis for committing of resources
### Points of Focus

| External Financial Reporting Objectives | • Complies with applicable accounting standards  
• Considers materiality  
• Reflects entity activities |
| External Non-Financial Reporting Objectives | • Complies with externally established standards and frameworks  
• Considers the required level of precision  
• Reflects entity activities |
| Internal Reporting Objectives | • Reflects management’s choices  
• Considers the required level of precision  
• Reflects entity activities |
Principle 6
Specifies Suitable Objectives (cont.)

Compliance Objectives

Points of Focus
- Reflects external laws and regulations
- Considers tolerances for risk
## Principle 6
Specifies Suitable Objectives (cont.)

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Identifying Financial Statement Accounts, Disclosures and Assertions</td>
<td>• Linking Accounts, Assertions, and Risks</td>
</tr>
<tr>
<td>• Specifying Financial Reporting Objectives</td>
<td>• Specifying Objectives</td>
</tr>
<tr>
<td></td>
<td>• Assessing the Suitability of Specified Objectives</td>
</tr>
<tr>
<td>• Assessing Materiality</td>
<td>• Assessing Materiality for a Private Company Financial Statement</td>
</tr>
<tr>
<td>• Reviewing and Updating Understanding of Applicable Standards</td>
<td>• Reviewing Financial Accounting Policies</td>
</tr>
<tr>
<td></td>
<td>• Reviewing and Updating Understanding of Applicable Standards</td>
</tr>
<tr>
<td></td>
<td>• Reviewing and Updating Statutory Reporting Requirements</td>
</tr>
<tr>
<td>• Considering the Range of Entity Activities</td>
<td>• Considering the Range of Assessment Activities</td>
</tr>
</tbody>
</table>
ICEFR Compendium - Example
Reviewing Financial Accounting Policies

• Celia Mendez is the controller of a $100 million biotechnology company. She reviews its accounting principles by considering:
  − Policies selected that are acceptable according to the applicable standards (US GAAP)
  − Situations where multiple acceptable alternatives are available and the rationale for selecting one policy over another
  − Differences in accounting policies from those of its peers
• Management discusses significant accounting policies with the audit committee on an annual basis.
Principle 7
Identify, Analyze and Respond to Risk

“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”

• Identifying and analyzing risks is an ongoing iterative process conducted to enhance the entity’s ability to achieve its objectives
• Management considers risks at all levels of the entity and takes the necessary actions to respond

<table>
<thead>
<tr>
<th>Points of Focus</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Includes entity, subsidiary, division, operating unit, and functional levels</td>
<td>Identify</td>
</tr>
<tr>
<td>• Analyzes internal and external factors; Involves appropriate levels of management; Estimates significance of risks identified</td>
<td>Analyze</td>
</tr>
<tr>
<td>• Determines how to respond to risks</td>
<td>Respond</td>
</tr>
</tbody>
</table>
**Principle 7**
Identify, Analyze and Respond to Risk (cont.)

<table>
<thead>
<tr>
<th>Summary of Enhanced Concepts of Principle 7:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Details that risk assessment includes risk identification, analysis, and response.</td>
</tr>
<tr>
<td>• Incorporates the concepts of inherent risk.</td>
</tr>
<tr>
<td>• Expands discussion regarding risk tolerance and how risk may be managed, including through acceptance, avoidance, reducing, and sharing risk.</td>
</tr>
<tr>
<td>• Considers velocity and persistence of risk (in addition to impact and likelihood).</td>
</tr>
<tr>
<td>• Incorporates consideration of outsourced service providers (OSPs).</td>
</tr>
</tbody>
</table>
## Principle 7
Identify, Analyze and Respond to Risk (cont.)

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Applying a Risk Identification Process</td>
<td>• Analyzing Risk Across Functions</td>
</tr>
<tr>
<td>• Assessing Risks to Significant Financial Statement Accounts</td>
<td>• Assessing Risks to Significant Financial Statement Accounts</td>
</tr>
<tr>
<td>• Meeting with Entity Personnel</td>
<td>• Using Risk Ratings</td>
</tr>
<tr>
<td>• Assessing the Likelihood and Significance of Identified Risks</td>
<td>• Analyzing Risk for Information Technology</td>
</tr>
<tr>
<td>• Considering Internal and External Factors</td>
<td>• Identifying and Responding to Risk</td>
</tr>
<tr>
<td>• Evaluating Risk Responses</td>
<td>• Using Benchmark Data to Assess Significance and Response to Risk</td>
</tr>
<tr>
<td></td>
<td>• Analyzing Risks from External Factors</td>
</tr>
<tr>
<td></td>
<td>• Considering Risk Response in a Revenue Process</td>
</tr>
</tbody>
</table>
ICEFR Compendium - Example
Analyzing Risk Across Functions

• The CFO holds a working session of department leaders from marketing, production, IT, HR, and administration to perform a risk analysis by department. Risks are rated from 1 (least risk) to 5 (most risk) based on potential impact on financial reporting and likelihood of occurrence. After the discussion sessions, the participants document the results in a table that outlines each specific risk together with the rating and factors contributing to the rating.
• Bailey Campbell, the controller for Center Bay Packing, assesses the risk relating to completeness of revenue. The company has grown over the past five years and now has annual revenues in excess of $50 million. Currently, Center Bay relies on a paper-based-bill-of-lading system. Delivery is deemed to have occurred when the bill of lading is signed by the customer as evidence that the goods have been received.

• Ms. Campbell has noted instances in the past year where shipping documentation was not provided to the finance department in a timely manner, sometimes as late as two weeks after the shipment was completed. These delays have resulted in misstatement of revenue. Ms. Campbell has determined that the risk related to revenue completeness need to be further reduced, and so she has decided to implement a bar-code scanner shipment system to track and capture shipping and revenue.
Principle 8
Assesses Fraud Risk

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

• The following points of focus highlight important characteristics relating to this principle:

<table>
<thead>
<tr>
<th>Points of Focus:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Considers various types of fraud</td>
</tr>
<tr>
<td>• Assesses incentive and pressures</td>
</tr>
<tr>
<td>• Assesses opportunities</td>
</tr>
<tr>
<td>• Assesses attitudes and rationalization</td>
</tr>
</tbody>
</table>
## Principle 8
Assesses Fraud Risk (cont.)

<table>
<thead>
<tr>
<th>Summary of Enhanced Concepts of Principle 8:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorporates the concept of fraud risk assessment.</td>
</tr>
<tr>
<td>Considerations related to various types of fraud, including fraudulent financial reporting, fraudulent non-financial reporting, misappropriation of assets, management override, safeguarding of assets, and corruption.</td>
</tr>
<tr>
<td>Evaluating incentives and pressures, opportunities, and attitudes and rationalizations.</td>
</tr>
<tr>
<td>Incorporates considerations of OSPs</td>
</tr>
</tbody>
</table>
Principle 8
Assesses Fraud Risk (cont.)

As part of the risk assessment process, organizations should identify the various ways that fraudulent financial reporting can occur, considering:

- Management bias, for instance in selecting accounting principles
- Degree of estimates and judgments in external reporting
- Fraud schemes and scenarios common to the industry sectors and markets in which the entity operates
- Geographic regions where the entity does business
- Incentives that may motivate fraudulent behavior
- Nature of technology and management’s ability to manipulate information
- Unusual or complex transactions subject to significant management influence
- Vulnerability to management override and potential schemes to circumvent existing control activities
### Principle 8
Assesses Fraud Risk (cont.)

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Conducting Fraud Risk Assessments</td>
<td>• Assessing Fraud Risk</td>
</tr>
<tr>
<td>• Considering Approaches to Circumvent or Override Controls</td>
<td>• Maintaining Oversight</td>
</tr>
<tr>
<td>• Considering Fraud Risk in the Internal Audit Plan</td>
<td>• Identifying and Analyzing Risk of Material Omission and Misstatement Due to Fraud</td>
</tr>
<tr>
<td>• Reviewing Incentives and Pressures Related to Compensation Programs</td>
<td>• Analyzing Compensation Structure</td>
</tr>
</tbody>
</table>
The chief compliance officer at a global retail operation, annually conducts a fraud risk assessment. In doing so, he interviews management at all the international locations about fraud issues. He analyzes:

- Historical fraud, including theft of inventory and the processes in place to identify and record such theft
- The methodology used for recording and calculating inventory and shrinkage
- Whistle-blower reports
- The number of manual entries vs. automated entries recorded
- The number of late entries due to subjective estimates

With this information, the chief compliance officer:

- Forms a preliminary view of the potential fraud activities, which he discusses with management of each jurisdiction in order to consider implications and what control activities can reduce the risk of fraud.
- Has discussions with human resources personnel and reviews information in the staff files.
- Uses his historical knowledge and staff information to assess the attitude of the local management toward the tolerance of fraud and to determine whether local management may rationalize fraudulent activities, including corruption.
- Once complete, submits a report to the audit committee for its consideration.
ICEFR Compendium - Example
Identifying and Analyzing Risk of Material Omission and Misstatement Due to Fraud

• Divisional controllers at consumer products company with locations in several countries, work with business unit leaders to identify and assess potential fraud risks.

• These risks are prioritized and categorized into various components, including risks of inventory theft, manipulation of data and bias in the development of accounting estimates, and other potential means of overriding controls.

• Internal audit reviews the resulting fraud risks and provides its point of view. In addition, the company meets with its external auditor to discuss the fraud risks to determine if there are others that should be under consideration. Business unit management plans responses and then selects and develops controls to mitigate these fraud risks.
Principle 9
Identifies and Analyzes Significant Change

“The organization identifies and assesses changes that could significantly impact the system of internal control.”

- The following points of focus highlight important characteristics relating to this principle:

  **Points of Focus:**
  - Assesses changes in the external environment
  - Assesses changes in the business model
  - Assesses changes in leadership

- **Summary of Enhanced Concepts of Principle 9:**
  Importance of assessing changes in the external environment, business model, operations, technology, relationship with OSPs, leadership and how such changes may impact internal control.
### Principle 9
Identifies and Analyzes Significant Change (cont.)

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Assessing Change in the External Environment</td>
<td>• Reacting to Significant Change Caused by External Factors</td>
</tr>
<tr>
<td>• Conducting Risk Assessments Relating to Significant Change</td>
<td>• Updating Risk Assessments For a New CEO</td>
</tr>
<tr>
<td>• Considering Change through Succession</td>
<td>• Responding to Significant Change from International Exposure</td>
</tr>
<tr>
<td>• Considering CEO and Senior Executive Changes</td>
<td>• Responding to Significant Change from an Acquisition</td>
</tr>
<tr>
<td></td>
<td>• Planning for Executive Transition</td>
</tr>
<tr>
<td></td>
<td>• Preparing for a Change in CEO</td>
</tr>
</tbody>
</table>
ICEFR Compendium - Example
Responding to Significant Change from International Exposure

- Consecutive Corp., a multi-billion-dollar technology equipment manufacturer that has historically focused on sales in the United States, has decided to expand internationally with both sales and manufacturing. As part of the expansion plans, Consecutive has assessed several factors:
  - Incremental revenue opportunities
  - Competition in the marketplace
  - Cultural dynamics of the targeted international location
  - Different laws and regulations, including those that would affect the company’s ability to defend its patents
  - Risk of increased fraud from theft and corruption
ICEFR Compendium - Example
Responding to Significant Change from International Exposure (cont.)

• Each of these factors presents incremental risks to financial reporting and processes that need to be managed. Therefore, Consecutive’s corporate controller is performing a risk assessment with the finance teams in the international locations to ensure these new risks are identified and to help management determine how best to respond.
Principles 6 - 9
Practical Application Examples

- Risk and control knowledge bases: Map the relevant assertions and risks to the material accounts, processes, and controls.

- Industry based risk maps: Identify the risks, both external and internal, across functions, that are most relevant for a company operating within your industry.

- Annual risk assessment, and prioritization: Analyze and prioritize identified risks based on the impact and vulnerability, including changes to people, process or technology.
Module 7
Control Activities
Module 7 - Agenda

• Control Activities Overview

• Discussion of Principles
  – Points of Focus
  – Enhanced Aspects
  – ICEFR Approaches and Examples
Control Activities Overview

10. Selects and Develops Control Activities

11. Selects and Develops General Controls over Technology

12. Deploys through Policies and Procedures

Principles of Component
Principle 10
Selects and Develops Control Activities

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

• The following points of focus highlight important characteristics relating to this principle:

<table>
<thead>
<tr>
<th>Points of Focus</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Integrates with Risk Assessment</td>
</tr>
<tr>
<td>• Considers Entity-Specific Factors</td>
</tr>
<tr>
<td>• Determines Relevant Business Processes</td>
</tr>
<tr>
<td>• Evaluates a Mix of Control Activity Types</td>
</tr>
</tbody>
</table>
Principle 10
Selects and Develops Control Activities (cont.)

Summary of Enhanced Concepts of Principle 10:

• The linkage between risk assessment and control activities.

• The types of controls applied (including considering preventive vs. detective controls).

• Differentiates between business process control activities and transaction control activities.

• Consideration of the level at which control activities are applied (including various levels of the organization).
Principle 10
Selects and Develops Control Activities (cont.)

**ICEFR Approaches**
- Using Matrices, Workshops, or an Inventory of Control Activities to Map Identified Risks to Control Activities
- Implementing or Assessing Control Activities when Outsourcing to a Third Party
- Considering the Types of Control Activities
- Identifying incompatible functions
- Considering Alternative Control Activities to the Segregation of Duties

**ICEFR Examples**
- Using an inventory of risks and control activities
- Obtaining a Report on Controls at a Service Organization from a Service Payroll Provider
- Evaluating Preventive versus Detective Control Activities
- Manually Assessing Incompatible Functions Across an Entity
- Using Alternative Control Activities when Access to Purchasing Transactions Are Not Segregated
ICEFR Compendium - Example
Obtaining a Report on Controls at a Service Organization from a Service Payroll Provider

ABC Company uses a third-party service to process payroll, which is considered significant to the company’s financial reporting because employee costs are a large part of their expenses. ABC Company obtains an SSAE16 (SOC1) report on controls from its third-party vendor, and reviews:

- Whether the described control objectives and control activities performed impact internal control over external financial reporting related to existence, completeness, and valuation of payroll expense
- The test results in the report and whether any exceptions have been identified
- Whether the period covered by the report is appropriate
- The control activities that it is expected to have in place in its own organization (as specified by the user control activities in the SSAE 16 report) to verify they are implemented and operating as intended
**Principle 11**
Selects and Develops General Controls over Technology

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

- The following points of focus highlight important characteristics relating to this principle:

<table>
<thead>
<tr>
<th>Points of Focus</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Dependency between the Use of Technology in Business Process and Technology General Controls</td>
</tr>
<tr>
<td>• Establishes Relevant Technology Infrastructure Control Activities</td>
</tr>
<tr>
<td>• Establishes Relevant Security Management Process Control Activities</td>
</tr>
<tr>
<td>• Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities</td>
</tr>
</tbody>
</table>
Principle 11
Selects and Develops General Controls over Technology (cont.)

Summary of Enhanced Concepts of Principle 11:

- Incorporates updated technology concepts, including those related to technology infrastructure, security, acquisition, development, maintenance, and use of Outsourced Service Providers (OSPs).
- Discusses the relationship between automated control activities and general information technology controls.
## Principle 11
Selects and Develops General Controls over Technology (cont.)

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Using Risk and Control Matrices to Document Technology and Dependencies</td>
<td>• Using a Walkthrough to Understand Technology Dependencies</td>
</tr>
<tr>
<td>• Evaluating End-User Computing</td>
<td>• Evaluating Financial Close End-User Spreadsheet Control Activities</td>
</tr>
<tr>
<td>• Implementing or Assessing Control Activities when Outsourcing IT Functions to a Third Party</td>
<td>• Obtaining a Report on Controls at a Service Organization from a Cloud-Based Service Provider</td>
</tr>
<tr>
<td>• Administering Security and Access</td>
<td>• Establishing Logical Security</td>
</tr>
</tbody>
</table>
### Principle 11
Selects and Develops General Controls over Technology (cont.)

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Configuring the IT Infrastructure to Support Restricted Access and Segregation of Duties</td>
<td>• Configuring the IT Infrastructure to Support Restricted Access and Segregation of Duties</td>
</tr>
<tr>
<td>• Configuring IT to Support Complete, Accurate, and Valid Processing of Transactions and Data</td>
<td>• Configuring IT to Support Complete, Accurate, and Valid Processing of Transactions and Data</td>
</tr>
<tr>
<td>• Applying a System Development Life Cycle over Packaged Software</td>
<td>• Managing Changes to Packaged Software</td>
</tr>
<tr>
<td>• Applying a System Development Life Cycle over Software Developed In-House</td>
<td>• Managing Changes to Custom Software</td>
</tr>
</tbody>
</table>
ICEFR Compendium - Example
Evaluating Financial Close End-User Spreadsheet Control Activities

• Smythe & Smythe International recently evaluated the use of spreadsheets in its financial close process. In doing so, it identified that the spreadsheets supporting the calculation of LIFO (last-in, first-out) adjustment and the fair values of goodwill, intangible assets and debt were high risk, based on the susceptibility of error and significance to the financial statements.

• Smythe & Smyth also classified the spreadsheets as high in complexity because they included the use of macros and multiple supporting spreadsheets to which cells and value were interlinked. The spreadsheets were used either as a basis for journal entries into the general ledger (LIFO Reserves) or as financial statement disclosures (fair value of goodwill, intangible assets, and debt).
ICEFR Compendium - Example
Evaluating Financial Close End-User Spreadsheet Control Activities

• The company considered the security, maintenance, and update risks of the spreadsheets and then selected and developed the following control activities:
  
  • **Input Control** – Input data is reconciled to source documentation to cover its completeness and accuracy.
  
  • **Access Control** – File-level access to the spreadsheets on a central server is limited to approved users, and a password is required to access the LIFO reserve spreadsheet.
  
  • **Version Control** – Standard naming conventions and directory structures are in place so only current and approved versions of spreadsheets are used.
  
  • **Calculation Testing** – When changes to formulas are made they are tested against a manual calculation for accuracy. All spreadsheet formulas are checked for accuracy at least once a year.
  
  • **Overall Analytics** – Analytical business process reviews using pre-established thresholds based on operating income and working capital function as a detective control to find errors in any of the spreadsheets.
ICEFR Compendium - Example
Configuring IT to Support Complete, Accurate, and Valid Processing of Transactions and Data

The IT operations staff of ABC Company monitors the batch and real-time processing of applications (including all financially significant applications) for errors using automated software. The scheduling software on the mainframe application checks for various problems with batch jobs, including data errors or programs that don’t complete properly or that run out of order. The operators are alerted to any of these issues and alert the appropriate business process owner based on standard documented procedures. For applications that process in real time, software is also used to automatically monitor for errors, such as incomplete, inaccurate, or invalid record transfers between systems. When a possible error is detected, the software attempts to resend the record without error. If the error persists, an email alert is sent to an operator who corrects the error following standard documented procedures. Management is notified of any errors in a weekly report which is reviewed to determine if any accounting record adjustments are required due to the system problems.
Principle 12
Deploys through Policies and Procedures

“The organization deploys control activities through policies that establish what is expected and procedures that put policies into action”

- The following points of focus highlight important characteristics relating to this principle:

<table>
<thead>
<tr>
<th>Points of Focus</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Establishes Policies and Procedures to Support Deployment of Management’s Directives</td>
</tr>
<tr>
<td>• Establishes Responsibility and Accountability for Executing Policies and Procedures</td>
</tr>
<tr>
<td>• Performs in a Timely Manner</td>
</tr>
<tr>
<td>• Takes Corrective Action</td>
</tr>
<tr>
<td>• Performs Using Competent Personnel</td>
</tr>
<tr>
<td>• Reassesses Policies and Procedures</td>
</tr>
</tbody>
</table>
Principle 12
Deploys through Policies and Procedures (cont.)

Summary of Enhanced Concepts of Principle 12:

- Establishing policies and procedures to support deployment of management’s directives.
- Establishing responsibility and accountability for executing policies and procedures.
- Reassessing policies and procedures on a periodic basis to determine their continued relevance and if revisions are needed.
<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Developing and Documenting Policies and Procedures</td>
<td>• Performing Control Activities in a Timely Manner</td>
</tr>
<tr>
<td>• Deploying Control Activities through Business Unit or Functional Leaders</td>
<td>• Deploying Control Activities through a Central Control Function</td>
</tr>
<tr>
<td>• Conduction Regular and Ad Hoc Assessments of Control Activities</td>
<td>• Regularly Assessing Policies and Procedures</td>
</tr>
</tbody>
</table>
ICEFR Compendium - Example
Regularly Assessing Policies and Procedures

Central Community Bank maintains a policy checklist on its intranet. The checklist references all the pertinent company policies and management's last review date, next reviews date, and board of director review and approval as applicable. The policies and procedures are reviewed annually or more frequently, in response to changes in underlying business processed. The internal audit department assesses compliance with company policy and procedures in conjunction with its internal audit reviews.
Module 8
Information and Communication
Module 8 - Agenda

• Information and Communication Overview

• Discussion of Principles
  – Points of Focus
  – Enhanced Aspects
  – ICEFR Approaches and Examples
Information & Communication

Principles of Component

13. Uses Relevant, Quality Information

14. Communicates Internally

15. Communicates Externally
Principle 13
Uses Reliable, Quality Information

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

- The following points of focus highlight important characteristics relating to this principle:

<table>
<thead>
<tr>
<th>Points of Focus</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Identifies Information Requirements</td>
</tr>
<tr>
<td>• Captures Internal and External Sources of Data</td>
</tr>
<tr>
<td>• Processes Relevant Data into Information</td>
</tr>
<tr>
<td>• Maintains Quality throughout Processing</td>
</tr>
<tr>
<td>• Considers Costs and Benefits</td>
</tr>
</tbody>
</table>
## Principle 13
Uses Reliable, Quality Information (cont.)

<table>
<thead>
<tr>
<th>Summary of Enhanced Concepts of Principle 13:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Identifying information requirements, verifying sources of data, processing relevant data, maintaining quality through processing, and using OSPs.</td>
</tr>
<tr>
<td>• Considering the costs and benefits of information as well as the impact of technology.</td>
</tr>
<tr>
<td>• Considering reliability and protection of data.</td>
</tr>
<tr>
<td>• Reevaluating information needs.</td>
</tr>
<tr>
<td>• Considering how information supports the functioning of internal control.</td>
</tr>
</tbody>
</table>
**Principle 13**
Uses Reliable, Quality Information (cont.)

- Quality of information depends on:
  - Accessible
  - Correct
  - Current
  - Protected
  - Retained
  - Sufficient
  - Timely
  - Valid
  - Verifiable

- Management establishes information management policies with clear responsibility and accountability for the quality of information
### Principle 13
Uses Reliable, Quality Information (cont.)

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Creating an Inventory of Information Requirements</td>
<td>• Evaluate Business Activities</td>
</tr>
<tr>
<td>• Obtaining Information from External Sources</td>
<td>• Maintain data flow diagrams, flow charts, narratives, and procedure manuals</td>
</tr>
<tr>
<td>• Obtaining information from Non-Finance management</td>
<td>• Gathering information from External Sources</td>
</tr>
<tr>
<td></td>
<td>• Capturing Information from Electronic Data Interchange</td>
</tr>
<tr>
<td></td>
<td>• Conducting quarterly interviews of operations and other management</td>
</tr>
<tr>
<td></td>
<td>• Obtaining operating information for financial reporting</td>
</tr>
</tbody>
</table>
**Principle 13**  
Uses Reliable, Quality Information (cont.)

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Creating and Maintaining information Repositories</td>
<td>• Use a data warehouse to facilitate access to information</td>
</tr>
<tr>
<td>• Using an Application to process data into information</td>
<td>• Data Capture and processing for the purchasing and payables cycle</td>
</tr>
<tr>
<td>• Enhancing Information Quality through a Data governance program</td>
<td>• Validating data and information</td>
</tr>
<tr>
<td>• Identifying, securing, and retaining financial information</td>
<td>• Identifying and protecting financial data and information</td>
</tr>
<tr>
<td></td>
<td>• Identifying and classifying data for financial reporting</td>
</tr>
</tbody>
</table>
ICEFR Compendium - Example
Validating Data and Information

• RightChoice Pharmacy, Inc. obtains significant data under-lying transactions recorded in point-of-sale systems located at each retail store. This data is immediately sent to the credit card company and to RightChoice’s internal data warehouse. A reconciliation is performed based on reports from this data warehouse to the payments due to the credit card companies.

• The CIO and credit/collections manager implemented continuous transaction monitoring software to support their data and information quality efforts. This software helps them verify their accounts receivable balances daily (avoiding time consuming month-end reconciliations).

• Targeted data queries allow the software to identify duplicate entries, unusual transactions, missing data, and incomplete data transfers.

• Continuous monitoring software enables data analysis used to support control activities to detect potential indicators of fraud.
Principle 14
Communicates Internally

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

• The following points of focus highlight important characteristics relating to this principle:

**Points of Focus:**

- Communicates Internal Control Information
- Communicates with the Board of Directors
- Provides Separate Communication Lines
- Selects relevant Method of Communication
Principle 14
Communicates Internally

Enhanced Aspects of Principle 14:

- Importance of communication between management and the board of directors such that both have sufficient information to successfully fulfill their roles
- Providing separate channels of communication for anonymous or confidential communication when normal communication channels are inoperative or ineffective (e.g., through whistle-blower hotlines).
Principle 14
Communicates Internally (cont.)

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Communicating information regarding External Financial Reporting Objectives and Internal control</td>
<td>• Using Communication Programs to Reinforce Internal Control</td>
</tr>
<tr>
<td></td>
<td>• Using an Internal Accounting and Finance Conference to Reinforce Policy Changes</td>
</tr>
<tr>
<td>• Communicating Internal Control responsibilities</td>
<td>• Using Governance, Risk, and Compliance Technology to Manage Internal Controls</td>
</tr>
<tr>
<td>• Developing guidelines for communication to the Board of Directors</td>
<td>• Facilitating Communication between Executive Management and the Board of Directors</td>
</tr>
<tr>
<td>• Reviewing Financial and Internal Control information with Board of Directors</td>
<td>• Preparing Financial and Internal Control Reporting Package for Discussion with the Board</td>
</tr>
</tbody>
</table>
## Principle 14
Communicates Internally (cont.)

### ICEFR Approaches
- Communicating a Whistle-Blower Program to Company Personnel
- Communicating through Alternative Reporting Channels
- Establishing Cross-Functional and Multidirectional Internal Control Communication Processes and forums

### ICEFR Examples
- Employee Ethics Hotline
- Establishing a Mentoring Program to Encourage Communicating with Management
- Establishing a Cross-Functional Internal Control Committee
ICEFR Compendium - Example
• Using an Internal Accounting and Finance Conference to Reinforce Policy Changes

NetComm, Inc., a broadband infrastructure company, holds a semi-annual meeting led by the CFO and controller. The personnel from the finance department attend these meeting to obtain updated information on significant new or changed matters that impact finance activities and financial results. Meeting topics routinely include:
• Key objectives for the next six months
• Reinforcement of the company’s policies related to ethics and integrity
• Expectations regarding findings from internal or external audits related to financial reporting and control
• Changes to the internal control structure
• Significant recent or anticipated events such as the sale of a business, acquisition of assets, restructuring of operations, or introduction of a new product
• Changes to accounting policy and regulatory rules that would impact how the company processes its financial transactions and produces its financial reports
**Principle 15**
Communicates Externally

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

- The following points of focus highlight important characteristics relating to this principle:

<table>
<thead>
<tr>
<th>Points of Focus:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Communicates to External Parties</td>
</tr>
<tr>
<td>• Enables Inbound Communications</td>
</tr>
<tr>
<td>• Communicates with the Board of Directors</td>
</tr>
<tr>
<td>• Provides Separate Communication Lines</td>
</tr>
<tr>
<td>• Selects Relevant Method of Communication</td>
</tr>
</tbody>
</table>
## Principle 15
Communicates Externally

### Enhanced Aspects of Principle 15:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Importance of open communication channels to allow input from stakeholders, including external party assessment results, to the board of directors.</td>
</tr>
<tr>
<td>2.</td>
<td>Providing separate channels of communication for anonymous or confidential communication when normal communication channels are inoperative or ineffective (e.g., through whistle-blower hotlines).</td>
</tr>
<tr>
<td>3.</td>
<td>Considerations related to OSPs.</td>
</tr>
</tbody>
</table>
### Principle 15
Communicates Externally (cont.)

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Communicating information regarding to Relevant External Parties</td>
<td>• Communicating Internal Control Information to a Federal Agency</td>
</tr>
<tr>
<td>• Obtaining Information from Outside Sources</td>
<td>• Establishing Periodic Communications with Contractors and Outsource Service Providers</td>
</tr>
<tr>
<td>• Surveying External Parties</td>
<td>• Communications from Regulatory Bodies</td>
</tr>
<tr>
<td>• Communicating the Whistle-Blower Program to Outside Parties</td>
<td>• Obtaining information from External Sources to Assist with Accounting Estimates</td>
</tr>
<tr>
<td>• Reviewing External Audit Communications</td>
<td>• Conducting Discussions with Customers</td>
</tr>
<tr>
<td></td>
<td>• Facilitating Communication with External Parties</td>
</tr>
<tr>
<td></td>
<td>• Managing and Assessing External Audit Communications</td>
</tr>
</tbody>
</table>
ICEFR Compendium - Example
Establishing Periodic Communications with Contractors and Outsource Service Providers

- Confab Group, a private Telecommunications company, outsources all of its manufacturing activities to third parties around the world. Confab is responsible for damage or loss of inventory from the receipt of raw materials at the third-party manufacturer until completed products are delivered to freight forwarder for shipment. Therefore the company retains a significant risk to inventory that is not within its physical control. Confab has specific policies and procedures for purchasing, manufacture and preparation of shipments to mitigate its exposure and to support estimates for inventory reserves. These policies are communicated to manufacturers along with contract clauses to adhere to these polices and the right to audit by the company
ICEFR Compendium - Example
Establishing Periodic Communications with Contractors and Outsource Service Providers (cont.)

• In order to ensure the policies and procedures are followed, Confab has implemented the following:
  − Website to communicate with the contract manufacturers
  − A link to the policies and procedures which contractors are required to acknowledge they have read and understood the polices
  − Periodic reports from the manufactures on the inventory balances
  − Periodic onsite audits of the contract manufacturers
  − Confab also performs annual reviews of the contract manufacturers controls that support the completeness and accuracy of reports provided throughout the year.
Discussion Question

What controls are in place to ensure the quality and integrity of information produced by the entity?

Has management considered whether monitoring/review type controls are sufficiently precise to prevent/detect a material misstatement?
Module 9
Monitoring
Module 9 - Agenda

- Monitoring Overview and Concepts
- Discussion of Principles
  - Points of Focus
  - Enhanced Aspects
  - ICEFR Approaches and Examples
- COSO’s Guidance on Monitoring Internal Control Systems
Monitoring Overview

16. Selects, develops and performs evaluations to determine if components of IC are present and functioning

17. Evaluates and communicates IC deficiencies

Principles of Component
Monitoring Activities Overview and Concepts

“Monitoring activities assess whether each of the five components of internal control and relevant principles is present and functioning”

• Monitoring is a key input of the organization’s assessment of the effectiveness of internal control
  − Provides valuable support for assertions of the effectiveness of the system of internal control

• Monitoring activities are selected, developed, and performed to ascertain whether each component continues to be present and functioning or if change is needed
  − Where appropriate, monitoring activities identify and examine expectation gaps relating to anomalies and abnormalities
  − When reviewing and investigating expectation gaps, management often identifies root causes of such gaps
Principle 16
Conducts Ongoing and/or Separate Evaluations

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

- The following points of focus highlight important characteristics relating to this principle:

<table>
<thead>
<tr>
<th>Points of Focus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Considers a mix of ongoing and separate evaluations</td>
</tr>
<tr>
<td>Considers rate of change</td>
</tr>
<tr>
<td>Establishes baseline understanding</td>
</tr>
<tr>
<td>Uses knowledgeable personnel</td>
</tr>
<tr>
<td>Integrates with business processes</td>
</tr>
<tr>
<td>Adjusts scope and frequency</td>
</tr>
<tr>
<td>Objectively evaluates</td>
</tr>
</tbody>
</table>
Principle 16
Conducts Ongoing and/or Separate Evaluations (cont.)

Enhanced Aspects of Principle 16:

- Considering the rate of change when developing monitoring activities.
- Using a baseline of understanding of internal control to establish plans for ongoing and separate evaluations
- Considerations regarding monitoring at different levels of an organization and monitoring of outsourced service providers
- Using technology in the context of monitoring
Ongoing Monitoring vs. Separate Evaluations

**Ongoing Monitoring:**
- Typically closer to operation of controls
- Offers earliest opportunity to identify weakness
- Often represents routine supervisory activities or a “self-assessment” process performed at the business unit level

** Separate Evaluations:**
- Generally more objective
- Validate results of ongoing monitoring
- Often performed by an internal audit or other compliance group
- Typically risk-based; e.g. higher risk areas are tested more frequently
Principle 16
Conducts Ongoing and/or Separate Evaluations (cont.)

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Periodically Reviewing the Mix of Monitoring Activities</td>
</tr>
<tr>
<td>• Establishing a Baseline</td>
</tr>
<tr>
<td>• Identifying and Using Metrics</td>
</tr>
<tr>
<td>• Designing and Implementing a Dashboard</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Changes in Business Operations</td>
</tr>
<tr>
<td>• Changing the Internal Audit Plan</td>
</tr>
<tr>
<td>• Establishing a Baseline</td>
</tr>
<tr>
<td>• Using Metrics to Monitor Payroll</td>
</tr>
<tr>
<td>• Using Built-in Operating Measures and Key Control Indicators</td>
</tr>
<tr>
<td>• Using Dashboards to Relate Operating Information</td>
</tr>
</tbody>
</table>
# Principle 16
Conducts Ongoing and/or Separate Evaluations (cont.)

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Using Technology to Support Monitoring Activities</td>
<td>• Using Continuous Monitoring</td>
</tr>
<tr>
<td>• Conducting Separate Evaluations</td>
<td>• Using Technology to Identify Trends</td>
</tr>
<tr>
<td>• Using Internal Audit to Conduct Separate Evaluations</td>
<td>• Investigating and Reporting Whistle-blower Allegations</td>
</tr>
<tr>
<td>• Understanding Controls at an Outsourced Service Provider</td>
<td>• Identifying and Protecting Sensitive Financial Data and Information</td>
</tr>
<tr>
<td></td>
<td>• Conducting Senior Financial Officer Visits</td>
</tr>
<tr>
<td></td>
<td>• Using Self-Assessments</td>
</tr>
<tr>
<td></td>
<td>• Identifying and Analyzing Risk of Material Omission of Misstatement Due to Fraud</td>
</tr>
<tr>
<td></td>
<td>• Internal Audit Conducting Separate Evaluations</td>
</tr>
<tr>
<td></td>
<td>• Reviewing Service Auditor’s Report for Changes in Controls</td>
</tr>
</tbody>
</table>
ICEFR Compendium - Example
Changing the Internal Audit Plan

• Villiam Financial Services is a publicly held global company. Recently the industry has experienced significant rate of change because of increasing focus and complexity of the company's financial products. In response to these changes, Villam’s management and board of directors have reprioritized the activities conducted by its internal audit department, including:
  – More active oversight of Villam’s recently enhanced risk management and governance process
  – An iterative risk assessment process that performs a risk review annually and more often if the business changes
  – Reviews of financial and operations data to identify risks and adverse trends, and to respond to them accordingly by conducting targeted audits
ICEFR Compendium - Approach
Using Technology to Support Monitoring Activities

- Management uses technology to support the monitoring of the system of internal control in the ordinary course of business through automated monitoring applications.
- Management uses the automated monitoring application to efficiently and continuously review large volumes of data at a low cost with a high standard of objectivity (once programmed and tested). Automated monitoring activities may include:
  - Checking transactions against predefined thresholds for anomalies
  - Monitoring transactions for trends or patterns
  - Assessing automated performance indicators, metrics, and measures that may lead to improvements in process and business
Principle 17
Evaluates andCommunicates Deficiencies

“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”

• The following points of focus highlight important
characteristics relating to this principle:

<table>
<thead>
<tr>
<th>Points of Focus:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Assesses results</td>
</tr>
<tr>
<td>• Communicates deficiencies</td>
</tr>
<tr>
<td>• Monitors corrective actions</td>
</tr>
</tbody>
</table>
Principle 17
Evaluates and Communicates Deficiencies (cont’)

Enhanced Aspects of Principle 17:

• Communicating deficiencies
• Monitoring corrective actions
Principle 17
Evaluates and Communicates Deficiencies (cont.)

ICEFR
Approaches

• Assessing and Reporting Deficiencies
• Monitoring Corrective Action
• Developing Guidelines for Reporting Deficiencies

ICEFR
Examples

• Identifying Sources of Deficiencies
• Reporting Protocols for Identified Deficiencies

• Establishing Reporting Protocols for Identified Deficiencies [and Monitoring Remediation]
• Follow up Reporting on Internal Audit Issues

• Reporting Deficiencies to the Board
ICEFR Compendium - Approach
Assessing and Reporting Deficiencies

• Management develops policies and practices to periodically assess and communicate deficiencies that result from the entity’s monitoring activities and other sources.

• Management establishes a practice where all deficiencies in internal control over external financial reporting, regardless of materiality, are reported to the responsible manager at least one level of management above, both of whom are positioned to take or oversee corrective action.

• Management also classifies deficiencies for the further reporting to senior management or the board based on criteria established by standard setters or regulators....
Principles 16 and 17
Practical Application Examples

• Diagnostic and maturity model: Establish a “risk intelligent” baseline, from which changes can be identified, and management can establish a monitoring program.

• Continuous controls monitoring: Use automated data analytics tools and techniques to monitor selected transactions on a periodic basis based upon relative risk, or to identify changes and unusual trends.

• Controls status/deficiency dashboard, and risk and control matrices: Use to track the status of controls testing, internal audits, or various process evaluations as well as the results of those evaluations (for ease of tracking of action items and status reporting). Can also be used for reporting deficiencies to the audit committee of the board, and comparison to prior period results.
Discussion Questions

• What does your company do to monitor outsourced service providers or other elements of COSO?

• What does your company do to monitor non-significant components (i.e., those components not “in scope” for SOX or internal audit) which when aggregated may become material?

• Have you contemplated what changes, if any, will need to be made to your existing Internal Audit plan(s) given the planned adoption/implementation of COSO’s revised I/C framework?
Activity: Identify Component Controls

- Refer to Handout 2, which is the summary of Components, Principles and Points of Focus.
- Identify relevant controls that address the principles within the assigned component. Consider the points of focus to assist in the identification of relevant control activities.
- Flipchart the:
  - Relevant controls identified for each principle
  - Control gaps identified for each principle

Prepare Responses – 15 minutes
Debrief Responses – 20 minutes
Activity #1 – Flipchart Example

<table>
<thead>
<tr>
<th>COMPONENT: Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
</tr>
<tr>
<td>CA#1</td>
</tr>
<tr>
<td>CA#2</td>
</tr>
<tr>
<td>CA#3</td>
</tr>
<tr>
<td>n/a</td>
</tr>
</tbody>
</table>

Copyright © 2013 Deloitte Development LLC. All rights reserved.
Module 10
Considerations & Next Steps
Module 10 - Agenda

- Considerations & Next Steps: The 4-Step Approach
  - Step 1: Understand and Educate
  - Step 2: Assess
  - Step 3: Plan & Implement
  - Step 4: Communicate

- Recap

- The Opportunities
Considerations and Next Steps: The 4-Step Approach

Companies complying with Section 404 of the Sarbanes-Oxley Act of 2002 will be required to utilize the 2013 COSO framework by: December 15, 2014
1. Understand and Educate

<table>
<thead>
<tr>
<th>Understand</th>
<th>Educate</th>
<th>Training</th>
</tr>
</thead>
</table>
| • The impact of the 2013 Framework on management’s assessment of the effectiveness of ICEFR will depend on how a company applied and interpreted the concepts in the prior Framework. | • Management will need to assess their education needs in equipping the core team with COSO 2013 Framework knowledge. • Assess training needs and obtain required education to become SMEs in identifying:  
  • New concepts and Key changes  
  • SOX Compliance requirements  
  • Formulate goals and expectations to be realized at the completion of training | • Roll out a formal training program within the Company  
• Train Management on the 2013 framework using:  
  • AICPA Toolkit  
  • New 2013 COSO  
  • 2013 Illustrative tools  
  • ICEFR Compendium  
• Conduct and provide training to Management’s core team  
• Train IA function to consider recognizing other risks, apart from compliance and financial matters |

To appropriately assess the impact, management will need to **read and understand** the 2013 Framework and identify new concepts and changes.
2. Perform Assessment

**IA Function: Operations, Compliance & Reporting**

- Analyze the effectiveness of the IA function in meeting the requirements outlined in the revised Internal Control framework.
- Identify how to leverage the revised 2013 Internal Control Framework, specifically related to internal controls in non-financial reporting areas, operations and compliance.

**Gap Assessment**

- Identify potential gaps through assessment of current state of processes, control activities and available internal control documentation regarding meeting the 17 principles and related points of focus in the new framework.

**Risk Assessment**

- Assess the process followed and revise the frequency, focusing on Fraud risk assessment.
- Evaluate the integrity and quality of information.
- Monitoring and related oversight of key activities performed at the third-party service providers.
- Precision of higher level detective/review type controls activities.
3. Plan and Implement

Develop and Execute a Transition Plan for SOX Compliance

<table>
<thead>
<tr>
<th>Plan</th>
<th>Utilize</th>
<th>Implement</th>
</tr>
</thead>
</table>
| - Finalize the updated SOX compliance methodology and approach to be undertaken  
- Define project governance and decision rights within core team  
- Develop a detailed project plan with key milestones  
- Identify and assign resources  
- Confirm proper disclosure of the framework used during the transition period and at the time the 2013 Framework is adopted | - Utilize SMEs and the right talent with technical knowledge to identify and address the new concepts and key changes proposed in COSO’s revised I/C framework with respect to its Internal Audit function activities and related audit programs  
- Considering using activities performed in 2013 (e.g., walkthroughs, testing of relevant controls, evaluation of deficiencies) to identify necessary changes and pilot or field test the application of the 2013 Framework. | - Document & Evaluate: Update the format and/or flow of your underlying documentation, aligning it to the new mapping to 2013 COSO Framework  
- Validation Testing and Gap Remediation: Assess design, implement controls, improve control reporting, perform validation testing, identify gaps, remediate gaps.  
- External Review & Testing: Communicate with external auditor to assess environment, and test updated SOX compliance program. |
4. Communicate

**Internal**
Coordinate and communicate internally with all groups that are responsible for implementing, monitoring, and reporting on ICEFR (including Internal Audit)

**External**
Discuss and coordinate activities with external auditor.
Recap: Considerations and Next Steps

Understand and Educate
- Read 2013 Framework
- Identify new concepts and changes
- Consider training and education needs

Assess
- Assess and evaluate needs regarding control objectives for operations, compliance, and reporting
- Determine impacts on the entity’s design and evaluation of ICEFR
  - Assess coverage of the principles
  - Assess current processes, activities, and available documentation regarding meeting the principles
  - Identify any gaps

Plan and Implement
- Identify the steps that need to be performed to transition to the 2013 Framework
- Formulate a plan to transition by December 15, 2014
- Take appropriate steps to implement plan

Communicate
- Communicate internally with all groups responsible for evaluating, monitoring, and reporting on the organization’s internal control
- Discuss and coordinate activities with internal audit (if applicable) and the external auditor
The Opportunities

• The 2013 Framework provides a good opportunity to create value for your organization and refresh your internal control system.

• Improve anti-fraud programs, new corporate governance paradigms, IT systems and risks, outsourcing to third parties

• Refresh and enhance internal control
  – Synergies and simplifications may be available
  – May also identify gaps to be addressed
  – Improve operations, compliance, and reporting
Discussion Questions

• How do you plan to communicate the new COSO Framework to your organization?

• Has your organization thought about how they will educate and train their key people on the new COSO Framework?

• Other than the ones we have already discussed in previous activities, what gaps do you believe your organization will identify?
Module 11
Available Resources
Available Resources

External Resources
• COSO Official Site – www.coso.org
  – Read Press Release
  – Download Executive Summary
  – Read FAQs
  – Download PowerPoint Slides
  – Purchase Framework and Tools
  – COSO Risk Assessment in Practice Guide*
  – Monitoring Guidance Available
• AICPA
  – Toolkit
  – Management Override of Internal Control – The Achilles’ Heal of Fraud Prevention:
    http://www.aicpa.org/ForThePublic/AuditCommitteeEffectiveness/DownloadableDocuments/achillesheel.pdf
Available Resources

• Deloitte Publications – www.deloitte.com
  – Heads Up: COSO Enhances its Internal Control — Integrated Framework (6/10/13)
  – Heads Up: Update on the Project to Enhance COSO’s Internal Control — Integrated Framework (8/7/12)
  – Heads Up: COSO Releases Exposure Draft of Updated Integrated Framework on Internal Control (2/6/12)
COSO Risk Assessment in Practice

• Focuses on broader enterprise-wide risk management (ERM)

• Provides an overview of risk assessment approaches and techniques that have emerged as the most useful and sustainable for decision-making

• Available for download: http://www.coso.org/guidance.htm
COSO Monitoring Guidance

• The 2013 Framework does not change or supersede the Monitoring Guidance
• Intended to help organizations improve the effectiveness and efficiency of their monitoring component
• Provide practical guidance that illustrates how monitoring can be incorporated into an organization’s business
• Available for download: http://www.coso.org/guidance.htm
QUESTIONS