COSO/Internal Control
The Basics of Internal Auditing
October 9-10, 2014

Florida Rivera-Alsing
MBA, CIA, CPA, CISA, CFE, LIFA, CIDA, CRMA
Chief Audit Executive
State Board of Administration of Florida

Agenda
- Key concepts
- IIA standards
- Definition of internal control
- Objectives of internal controls
- Types of controls
- Frameworks
- Internal control deficiencies
- Limitation of internal controls
- Responsible for internal controls

Key Concepts
Concern of any entity?
RISKS
Anything that could negatively impact the entity’s ability to meet its business objectives
Key Concepts

How to mitigate the risks?

Implement Internal Controls

Internal Auditors’ Responsibility

IIA Std. 2130 – Control

The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

2130.A1 – The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization’s governance, operations, and information systems regarding the:

• Achievement of the organization’s strategic objectives;
• Reliability and integrity of financial and operational information;
• Effectiveness and efficiency of operations and programs;
• Safeguarding of assets; and
• Compliance with laws, regulations, policies, procedures, and contracts.

Committee of Sponsoring Org. of the Treadway Commission

COSO

AAA AICPA FEI IMA IIA
Definition of Internal Control

The IIA

"Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved."

Definition of Internal Control

AICPA (AU Section 325):

"Internal control is a process - effected by those charged with governance, management and other personnel - designed to provide reasonable assurance about the achievement of the entity's objectives with regard to the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations."

Definition of Internal Control

COSO

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 financial reporting
- Compliance with applicable laws and regulations"
Definition of Internal Control

Green Book

“Internal control is a process effected by an entity’s oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved.”

Internal Control Concepts

• Process
• Effected by people
• Reasonable assurance
• Achievement of objectives

Objectives of Internal Controls

- Reporting
- Operations
- Compliance
Objectives of Internal Controls

ACHIEVEMENT OF OBJECTIVES:

1. Operations – effectiveness and efficiency of operations
   Effective operations produce the intended results from operational processes, while efficient operations do so in a manner that minimizes the waste of resources.

Objectives of Internal Controls

ACHIEVEMENT OF OBJECTIVES:

2. Reporting – Reliability of reporting for internal and external use
   a. internal financial and non-financial reporting
   b. external financial and non-financial reporting.

Objectives of Internal Controls

ACHIEVEMENT OF OBJECTIVES:

3. Compliance – compliance with applicable laws and regulations
Examples of Internal Controls

Think about what you do
At home
Your ATM/Debit card
Your car

Think about what you do at work

Preventive vs. Detective

• Preventive – attempt to deter or stop an unwanted outcome before it happens.
  Examples: use of passwords, approval, policies, procedures

• Detective – attempt to detect errors or irregularities that may have already occurred.
  Examples: reconciliations, monitoring of actual expenses vs. budget, prior periods, forecasts

Hard vs. Soft

<table>
<thead>
<tr>
<th>Hard</th>
<th>Soft</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Formal</td>
<td>• Informal</td>
</tr>
<tr>
<td>• Tangible</td>
<td>• Intangible</td>
</tr>
<tr>
<td>• Examples:</td>
<td>• Examples:</td>
</tr>
<tr>
<td>Organizational structure</td>
<td>Tone at the Top</td>
</tr>
<tr>
<td>Policies</td>
<td>Ethical climate</td>
</tr>
<tr>
<td>Procedures</td>
<td>Integrity</td>
</tr>
<tr>
<td>Segregation of duties</td>
<td>Trust</td>
</tr>
<tr>
<td></td>
<td>Competence</td>
</tr>
</tbody>
</table>
**Manual vs. Automated**

- **Manual Controls** - manually performed; Could either:
  - solely manual where no IT generated reports are used or
  - IT-dependent where a system-generated report is used to test a particular control
- **Automated Controls** - performed entirely by the computer system

**Key vs. Secondary**

**Key** – those that must operate effectively to reduce the risk to an acceptable level

**Secondary** – those that help the process run smoothly, but are not essential

**Key Concepts**

1. To identify the correct control, you must know what risks are present.
2. To know what risks are present, you need to understand what objectives are being sought.
3. Therefore, Objectives ➔ Risks ➔ Controls
Key Concepts

The relationship between risk and control activities

$$\text{RISK} = \text{CONTROL}$$

The greater the risk, the greater the control needed

Control Framework

IIA Std. 2450 – Overall Opinions

When an overall opinion is issued, it must take into account the expectations of senior management, the board, and other stakeholders and must be supported by sufficient, reliable, relevant, and useful information.

Interpretation:
- The communication will identify:
  - The scope, including the time period to which the opinion pertains;
  - Scope limitations;
  - Consideration of all related projects including the reliance on other assurance providers;
  - The risk or control framework or other criteria used as a basis for the overall opinion;
  - The overall opinion, judgment, or conclusion reached.

The reasons for an unfavorable overall opinion must be stated.

• Criteria in the framework provide basis for:
  - Understanding control in an organization
  - Assessment about the effectiveness of control.

• Provide a standard review process
Control Framework

- COSO – major accounting and audit professional organizations
- CoCo - Canadian Institute of Chartered Accountants
- COBIT
- Green Book

COSO - Components of Internal Control

Control Environment
- Sets the tone
- Is the foundation for all other components
- Influences the effectiveness of I/C

COSO – Components and Principles of Internal Control

<table>
<thead>
<tr>
<th>Component</th>
<th>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. Board 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>
</tbody>
</table>
### COSO – Components and Principles of Internal Control

<table>
<thead>
<tr>
<th>Component</th>
<th>Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Assessment</strong></td>
<td>6. Specifies suitable 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><strong>Control Activities</strong></td>
<td>10. Selects and develops control activities to mitigate risks</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><strong>Information and communication</strong></td>
<td>13. Obtains, generates, uses relevant information</td>
</tr>
<tr>
<td></td>
<td>14. Communicates internally</td>
</tr>
<tr>
<td></td>
<td>15. Communicates externally</td>
</tr>
</tbody>
</table>

**Risk Assessment**
- Economic conditions, staffing changes, new systems, regulatory changes, natural disasters, etc. that threaten the accomplishment of objectives.

**Risk assessment** is the process of identifying, evaluating, and deciding how to manage these risk events...

- What is the likelihood of the event occurring?
- What would be the impact if it were to occur?
- What can we do to prevent or reduce the risk?

**Control Activities**
- Tools - policies, procedures, processes designed and implemented to help ensure that management directives are carried out.
- Help prevent or reduce the risks that can impede the accomplishment of objectives.
- Occur throughout the organization, at all levels, and in all functions.

**Information and communication**
- Pertinent information must be captured, identified, and communicated on a timely basis.
- Effective information and communication systems enable the organization’s people to exchange the information needed to conduct, manage, and control its operations.
Monitoring activities

- Internal control systems must be monitored to assess their effectiveness. Are they operating as intended?
- Ongoing monitoring is necessary to react dynamically to changing conditions. Have controls become outdated, redundant, or obsolete?
- Monitoring occurs in the course of everyday operations. It includes regular management and supervisory activities and other actions personnel take in performing their duties.

Principles

16. Selects, develops, performs ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies timely

Green Book

Written for government
- Leverages the COSO Framework
- Uses government terms

COSO’s 5 components, 17 principles, plus attributes

Effective beginning FY 2016
“A deficiency in internal control 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 and correct misstatements on a timely basis.”

(AICPA AU 325)
Limitations of Internal Controls

- Human judgment – can be faulty
- Human failure – errors, mistakes, etc.
- Ability to override internal control
- Cost/benefit constraints
- Obsolescence

Responsible for Internal Control

EVERYONE

Final Words

"Two things seemed pretty apparent to me. One was, that in order to be a (Mississippi River) pilot, a man had got to learn more than any one man ought to be allowed to know; and the other was, that he must learn it all over again in a different way every 24 hours."

(Mark Twain, Life on the Mississippi)
Questions?

References
The COSO website at www.coso.org
Options available:
• Buy the full 2013 Framework
• Buy the Internal Control Integrated Framework
• Buy the Internal Control – Integrated Framework, Internal Control over External Financial Reporting
• Buy a complete bundle package: Internal Control – Integrated Framework and Compendium Bundle

References
• The IIA – www.theiia.org
• AICPA – www.aicpa.org
• AICPA AU Section 325
• OMB Circular A-133
• Sarbanes Oxley Act of 2002
Thank you!!

Flerida Rivera-Alsing
Chief Audit Executive
State Board of Adm. of Florida
flerida.rivera-alsing@sbafla.com
(850) 413-1259