Developing Effective Internal Controls Using the COSO Model

Office of State Controller
Internal Controls in a COSO Environment Seminar
Raleigh, North Carolina  March 2007

Mark S. Beasley
Director, ERM Initiative and Professor of Accounting
North Carolina State University
Today’s Objectives

1. Why all the buzz about COSO?

2. What do we mean by “internal control”?

3. What are the key components for effective internal control?
Who is COSO?

The Committee of Sponsoring Organizations of the Treadway Commission

AICPA

The Institute of Internal Auditors

Institute of Management Accountants

American Accounting Association

Financial Executives International
Why all the recent fuss over Internal Controls?
Fraud!

Perception that effective internal controls help prevent and detect fraud.
Sarbanes-Oxley

• Section 404
  Annual management assessments of IC over financial reporting

• Section 302
  Quarterly certifications by CEO and CFO that they have
  Controls that material information is disclosed to them
  Evaluated the effectiveness of IC within prior 90 days
PCAOB Auditing Std No. 2

• Paragraph .13

Management is required to
“...base its assessment...on a suitable, recognized control framework established by a body of experts that follow due process procedures”

• Paragraph .14

In the United States, COSO’s *Internal Control-Integrated Framework*
“provides a suitable and available framework for purposes of management’s assessment”
Why All the Focus on IC?

Source: KPMG Fraud Survey
Today's Objectives

2. What do we mean by “internal control”?
COSO’s Definition

Internal control is

“a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives”
COSO’s View of IC
3 Categories of IC Objectives

Operations

Compliance

Financial Reporting
5 Components of IC

- Monitoring
- Information and Communication
- Control Activities
- Risk Assessment
- Control Environment
Internal Control as a Process

- Risk Assessment
- Control Environment
- Control Activities
- Information and Communication
- Monitoring
- Specify financial reporting objectives
Key Concept

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. Thus,

   - *Objectives* → *Risks* → *Controls*
3. What are the key components for effective internal control?
Risk Assessment

- Specify financial reporting objectives
- Risk Assessment
- Control Environment
- Control Activities
- Monitoring
- Information and Communication
Risk Assessment

- Precondition to controls is identifying risks
  Can’t determine needed controls without knowing risks
- Every entity faces risks
  Risks constantly evolve
- Need a systematic process for risk management
  Focused on both likelihood and consequence
Drivers of Internal Controls

- Strategic Objectives
- Business Processes
- Identified Risks

Threats

Internal Control
Financial Reporting Objectives

• Safeguarding of Assets

• Emphasize reliable and relevant reporting
  Transparent - reflect economic reality
  Timely
  Meet GAAP – minimum threshold

• Account and transaction level objectives
  5 Financial Statement Assertions
Analyzing Risks Across Transaction Flows

Transactions
- Cash disbursements
- Payroll services and disbursements
- Allocation and adjustments

Journals
- Cash disbursements journal
- Payroll journal
- General journal

Ledgers, Trial Balance, and Financial Statements
- General ledger and subsidiary records
- General ledger trial balance
- Financial statements
Control Environment

- Sets the “tone at the top”
  - Board and Senior Management driven
- Influences control consciousness of its people
  - Core to sound integrity and ethical values
- Emphasis on competencies and authorities
- Foundation for all other components of IC
Relationship to Other Components

Control environment

- Risk assessment
- Control activities
- Information and communication
- Monitoring
Core Themes

- **Sound integrity and ethical values are critical to IC**
  - Code of Conduct

- **Board and audit committee play a vital role**
  - Independence and financial expertise

- **Mgt’s philosophy and operating style support IC**
  - Actions consistent with Code of Conduct

- **Entities must retain individuals with competencies**
  - Commitment to acquiring needed competencies

- **Employees are assigned appropriate levels of authority**
  - Delegation is clear and accountable

- **Human resource practices demonstrate commitment to integrity, ethical behavior, and competence**
  - Screening done not just for employment, but also promotion
Subcomponents

Control Environment

- Integrity & Ethical Values
- Commitment to Competence
- Board & Audit Comm.
- Mgt Philosophy & Operating Style
- Organ. Structure
- Assignment of Authority Respon.
- Human Resource Policies & Procedure
Control Activities
Control Activities

- Represent responses to identified risks
  Don’t need a control if no corresponding risks

- Control activities are
  Actions taken to address risks of achieving objectives

- Occur at all levels of an organization
  Company-wide controls
  Business process specific tasks

- Consists of 2 aspects:
  Policy of what should be done
  Procedures to accomplish policy
## Example – Revenues

<table>
<thead>
<tr>
<th>Assertions</th>
<th>Policies &amp; Procedures That Ensure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exist/Occur</td>
<td>Recorded revenues actually earned</td>
</tr>
<tr>
<td>Completeness</td>
<td>Revenues earned are actually recorded</td>
</tr>
<tr>
<td>Rights/Oblig</td>
<td>Organization has rights to revenue receivables</td>
</tr>
<tr>
<td>Valuation/Alloc</td>
<td>Revenues recorded at correct amounts</td>
</tr>
<tr>
<td>Present/Discl</td>
<td>Revenue policies/terms disclosed properly</td>
</tr>
</tbody>
</table>
Categories of Control Activities

1. Adequate separation of duties
2. Proper authorization of transactions and activities
3. Adequate documents and records
4. Physical control over assets and records
5. Independent checks on performance
Adequate Segregation of Duties

- Asset
- Accounting/Custody
- Authorization/Record keeping
- IT/Duties of Trans.
Combinations of Control Activities

• Management uses a mix of
  Preventative controls
  Detective controls

• Combinations of
  Manual controls
  Automated controls
IT General and Application Controls

Risk of unauthorized change to application software

Cash receipts application controls

Sales applications controls

Payroll application controls

Other cycle application controls

Risk of unauthorized master file update

GENERAL CONTROLS

Risk of system crash

Risk of unauthorized processing
## Example of IT Controls

<table>
<thead>
<tr>
<th>General Controls</th>
<th>Application Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Organization</td>
<td>Access restriction to application</td>
</tr>
<tr>
<td>Physical/Logical Security</td>
<td>Input data validation against master file</td>
</tr>
<tr>
<td>Systems Development</td>
<td>Range or Limit Checks</td>
</tr>
<tr>
<td>Change Management</td>
<td>Sequence Checks</td>
</tr>
<tr>
<td>Backup Planning</td>
<td>Programmed edits – logic tests</td>
</tr>
</tbody>
</table>
Cost – Benefit Considerations

Impact from Risks

Costs of Implementing Controls
Information and Communication

- Information is needed to carry out responsibilities
  - Information
    - From Management
    - To Management

- Effective Communication is needed
  - More than just information flow
  - Key is understanding the messages

- Information & Communication needs to be controlled, too
Information Flow

- **Key elements – system must**
  
  Identify  
  Capture  
  Process  
  Distribute

- **Information based on**
  
  Internal and external sources
  
  Operational information used to develop financial information

- **Information used to control activities that support objectives**
Communication

• Has management developed
  Communications program to reinforce IC objectives?
  Communications strategy to enable each employee to understand IC responsibilities?
  Process to determine if information needed by employees is timely and accurate?
  Communication mechanism for employees to be aware of ethical and legal requirements?

• Does the entity have “fail-safe” mechanisms in case normal channels of communications are inoperative?

• Is the Board of Directors receiving needed information?
Monitoring

Specify financial reporting objectives

Risk Assessment

Control Environment

Control Activities

Information and Communication

Monitoring
Monitoring

• Internal control systems need to be monitored
  a/k/a – “Monitoring of controls”

• Focus – assessing quality of system performance
  More than just information flow
  Key is understanding the messages

• Nature of Monitoring
  Ongoing
  Separate Evaluations
Ongoing Monitoring

• **Built into operations**
  
  Some automated
  Focus on deviations from norms

• **Provide continual feedback on controls**
  
  Should lead to investigations
  May lead to system changes
Separate Evaluations

• Evaluate effectiveness of ongoing monitoring
  Objective look from time to time
  Scope based on significance of risks

• Objective and competent evaluator
  Internal audit plays vital role
Monitoring of All Elements
Bringing it All Together

- 5 Components of Internal Control Must Work Together
- Can’t have effective Internal Control if one component weak
The Big Picture

Internal control is:
- a process
- designed to achieve financial reporting objectives
- five components that work together

Control Environment
- Implement and operate control environment, setting the tone of the company

Risk Assessment
- Determine which risks could result in a material misstatement to financial statements
- Determine how each of the other components, both separately and together, support reliable financial reporting

Continuous Improvement
- Examine opportunities for improvement in control effectiveness and efficiency

Control Activities
- Implement and operate control activities, using a range of activities to reduce risk to objectives

Information and Communication
- Implement and operate information and communication to support internal control

Monitoring
- Implement and operate monitoring activities to help ensure that controls continue to operate properly over time

Specify financial reporting objectives
- Refine financial reporting objectives based on changes potentially impacting the business

Note: Figure above is taken from COSO’s “Internal Control over Financial Reporting - Guidance for Public Companies, Volume II: Guidance”.
Risk Assessment

Note: Figure above is taken from COSO’s “Internal Control over Financial Reporting - Guidance for Public Companies, Volume II: Guidance”.
Control Environment

Note: Figure above is taken from COSO's "Internal Control over Financial Reporting - Guidance for Public Companies, Volume II: Guidance".
Control Activities

Note: Figure above is taken from COSO's "Internal Control over Financial Reporting - Guidance for Public Companies, Volume II: Guidance".
Information and Communication Monitoring

Note: Figure above is taken from COSO's "Internal Control over Financial Reporting - Guidance for Public Companies, Volume II: Guidance".
4 Points of Internal Control Failure

1. Focus on 4 Points of Failure
   - Assumption it’s only the auditor’s job
2. 4 Points of Failure
   - Assumption it’s only the auditor’s job
   - Failure to link risks and controls
Failure #3

2. 4 Points of Failure
   - Assumption it’s only the auditor’s job
   - Failure to link risks and controls
   - Inadequate monitoring of controls
Failure #4

2. 4 Points of Failure

- Assumption it’s only the auditor’s job
- Failure to link risks and controls
- Inadequate monitoring of controls
- Ignoring reality – risk of management override is always present
Guidance – Volume I

- Provides a high level summary
- Summarizes recent developments, internal control challenges, and the costs and benefits associated with internal control
- Focuses on risk as a basis for developing internal control
- Introduces internal control as a process
Guidance – Volume II

- Focuses on twenty fundamental principles
- These principles are drawn from the original Internal Control – Integrated Framework
- These principles assist smaller businesses in achieving internal control in a cost-effective manner
Guidance – Volume II: Principles, Attributes, Approaches, and Examples

Sound integrity and ethical values, particularly of top management, are developed and understood and set the standard of conduct for financial reporting.

**Principle 1**
- Articulates Values
- Monitors Adherence
- Addresses Deviation

**Three Attributes**
- Articulating and Demonstrating Integrity and Ethics
- Informing Employees about Integrity and Ethics
- Demonstrating Commitment to Integrity and Ethics

**Three Approaches**
- Company Newsletter Reinforcing Integrity and Ethics
- Promoting Awareness of Ethical Behavior
- Etc…

**Six Examples**
- Articulates Values
- Monitors Adherence
- Addresses Deviation
Guidance – Volume III

• Contains illustrative tools to assist management in evaluating internal control

• Managers may use the illustrative tools in determining whether the company has effectively applied the principles

• It is expected that other managers will use Volumes II and III as a reference source for guidance in those areas of particular need

• This volume is now also available in a Word format
A Look Back at Today’s Objectives

1. Why all the buzz about COSO?
   Sarbanes-Oxley
   Good business sense

2. What do we mean by “internal control”?
   More than just “checks and balances”
   Responses to risks threatening objectives

3. What are the key components for effective internal control?
   Complex interactions of 5 core components
   Range from high-level actions to detailed processes
Internal Controls
Provide Bridge to Success

• For Organizations
  Reduce exposures to risks threatening strategy

• For You
  Now an expected core competency of management
Reality:
Internal control checklists must link to Risks
Fraud risk is more than the auditor’s responsibility
Monitoring of controls must occur on an ongoing basis
Management override is always present risk

Mark Beasley
Director – ERM Initiative and Professor of Accounting
NC State University