COSO – Internal Control Findings

September 17, 2014
Objectives

1. Understand how to use the Framework to identify internal control deficiencies/findings
2. Understand internal control deficiencies that should lead to findings
3. Understand the key elements of an internal control finding
4. Understand the process of evaluating and monitoring corrective action plans
5. Review the Top 10 Internal Control Findings
Overall Objective

“OK, I’m now going to read out loud every single slide to you, word for word, until you all wish you’d just die.”
Introduction

Why should we care about Internal Control Findings?
Why Should We Care About Internal Control Findings?

- **WorldCom** - $11 billion+ worth of fraudulent accounting entries, capitalized line costs rather than expensing caused $180 billion in losses to investors. Found by Internal Auditors → SOX.

- **Waste Management** - $1.7 billion in fake earnings due to inordinately long lived assets thus decreasing depreciation expense. Caught when new CEO and Management analyzed accounting records. Whistleblower hotline installed.
Why Should We Care About Internal Control Findings?

• **The Baptist Foundation of Arizona** – convinced 11,000 elderly church members to invest their life’s savings and retirement funds into bogus real estate investments using bogus for-profit companies. BFA’s actual losses reached $585 million.

• **Peregrine Systems**- $100 million of revenue overstated by recording inventory placed on consignment as actual sales. Large AR questioned by SEC.
Why Should We Care About Internal Control Findings?

- **Enron** – Shareholders lost $71 billion. Caused by keeping debt off of balance sheet. Identified by Whistleblower.

- **Tyco** - $150 million stolen by CEO and CFO; Income inflated by $500 million. Unapproved loans, executive bonuses, fraudulent stock sales. Uncovered by SEC and Manhattan DA.
Why Should We Care About Internal Control Findings?

• **HealthSouth** – Inflated earnings by $1.4 billion; fabricated transactions; sold $75 million in stock a day before the company posted a huge loss = SEC investigation.

• **ZZZ Best** – The president of ZZZ Best’s fraudulent insurance restoration/construction division, generated more than 10,000 bogus documents that created $300 million in fictitious reconstruction projects. Auditors looked at projects ZZZ Best did not own. ZZZ Best did not even have a construction license.
Why Should We Care About Internal Control Findings?

• **Dixon, Illinois** – Town Treasurer siphoned off $54 million into a secret “Reserve” bank account. Town made budget cuts and laid off employees.

• **Peregrine Systems** - $100 million of revenue overstated by recording inventory placed on consignment as actual sales. Large AR questioned by SEC.
Why Should We Care About Internal Control Findings?

• **Lehman Bros.** – Hid over $50 billion of loans disguised as sales. Sold toxic assets to Cayman Island Banks with agreement to buy them back, thus overstating cash and understating toxic assets. Caught due to BK.

• **Bernie Madoff** - $66.8 billion lost due to largest Ponzi Scheme ever. Investors paid returns out of their own or other’s money. After he told his sons, they turned him in.
Objective #1 – Understand how to use the Framework to identify internal control findings
Internal Control consists of these 5 interrelated components
The COSO Cube – Depicts Basic Internal Controls

**Specify objectives** with respect to operations, compliance and reporting.

Design and Implement a **control environment** that sets the tone for the organization and its commitments to actions which mitigate risk.

**Identify and assess the risks** that may prevent achieving the desired objectives.

Design and implement specific **control activities**, including authorizations, completeness tests, reconciliations and reviews, to further mitigate risks.

Develop an effective **information and communication process** to ensure parties understand their control responsibilities and that management receives information to facilitates investigation and decision making.

**Monitor** the effectiveness of its control implementation.
What Has Changed

• 2013 version explicitly states **17 principles** that represent fundamental concepts associated with the 5 components, as well as **77 points of focus** that support the 17 principles.
• Reflects increased relevance of **technology**
• Focus on **governance** concepts
• Expands **anti-fraud** considerations
• Expands **reporting** category(external, internal & non-financial)
New Framework

• Requires that:
  – Each of the 5 components and 17 principles is present and functioning
  – All 5 components operate together in an integrated manner
  – Or.......... There is a weakness in the system of internal controls
Internal Control Deficiency Defined

A shortcoming in one or more components and the relevant principle that reduces the likelihood that an entity can achieve its objectives.
Objective #1 - Review

**Objective** - Understand how to use the Framework to identify internal control findings.

**Summary** – Each of the 5 components of internal control and the 17 principles can be used to assess the functioning of internal controls; use 77 points of focus for guidance.
Objective #2 - Understand internal control deficiencies that should lead to findings
Component: Control Environment

- **Principle #1:** The organization demonstrates a commitment to **integrity** and **ethical values**.

- **Potential Findings:**
  - Absence of an *effective* Ethics Policy
  - Absence of an *effective* Code of Conduct
  - Absence of *effective* behavioral monitoring processes
Control Environment (cont.)

• **Principle #2:** The Governing Body/City Council demonstrates **independence from management** and **exercises oversight** of the development and performance of internal control.

• Potential Findings:
  – Lack of established IC oversight assignments
  – Lack of qualified, trained oversight personnel
  – Undue influence by management
Control Environment (cont.)

- Principle #3: Management establishes, with board oversight, structures, reporting lines and appropriate authorities and responsibilities in the pursuit of objectives.

- Potential Findings:
  - Absence of controls over subsidiaries/divisions
  - Lack of defined authority/responsibility (job descriptions, policies and procedures)
Control Environment (cont.)

• **Principle #4:** The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

• Potential findings:
  – Lack of adequate performance evaluation system
  – Ineffective recruiting or employee development programs (training?)
  – Lack of succession planning
Control Environment (cont.)

“That’s my performance review?! Two thumbs up?!”
Control Environment (cont.)

• **Principle #5:** The organization holds individuals accountable for their internal control responsibilities.

• **Potential findings:**
  – Failure to evaluate performance with respect to achieving internal control objectives
  – Lack of performance measures, incentives and rewards pertaining to internal control responsibilities
  – Failure to periodically evaluate performance measures, incentives and rewards for ongoing relevance
Control Environment (cont.)

“I’m a little concerned that most exit interviews consist largely of people smiling and flipping me the bird.”
Component: Risk Assessment

• **Principle #6:** The organization specifies objectives with sufficient clarity to enable the identification and assessment of related risks.

• **Potential findings:**
  – Operational objectives are not clearly defined
  – Operational objectives are not evaluated for risk exposure
  – Inadequate financial & non-financial reporting objectives
Risk Assessment (cont.)

• Potential findings (continued)
  – External financial reporting
    • Does not require compliance with applicable accounting standards (GAAP)
    • Does not reflect entity activities (is not comprehensive or accurate)
  – External non-financial reporting
    • Does not comply with externally established standards
    • Does not provide a useful level of precision
    • Does not accurately reflect the entity’s activities
Risk Assessment (cont.)

• Potential findings (continued)
  – Internal reporting
    • Does not fulfill management’s need for information
    • Does not address all appropriate activities/functions
    • Is not sufficiently precise
  – Compliance
    • Does not align with external laws and regulations
Risk Assessment (cont.)

- **Principle #7:** The entity **identifies risks** to the achievement of its objectives and analyzes risks to determine how the risks should be **managed**.

- **Potential findings:**
  - Risk identification does not include **entity, division, operating unit & functional levels**
  - Risk assessment does not involve appropriate levels of management
  - The significance of risks are not estimated
  - Organization does not consider how to respond to risks
Maybe NEXT time you’ll hand the Risk Assessment in ON TIME!
**Risk Assessment (cont.)**

- **Principle #8:** The organization considers the potential for **fraud** in assessing risks to the achievement of objectives.

- **Potential findings:**
  - Fraud risk assessment process is absent or fails to consider the various types of fraud
  - Fails to assess incentives and pressures
  - Fails to assess opportunities
Indicators of Fraud Risk

• Conditions threaten entity’s financial stability
• Nature of the entity’s operations
• Management’s monitoring of compliance is inadequate
• Organization structure is unstable or unnecessarily complex
• Communication by management is lacking
• Management’s willingness to accept high levels of risk in making significant decisions
Indicators of Fraud Risk (cont.)

• Operating Policies & Procedures have not been developed or are outdated
• Key documentation is lacking, or nonexistent
• Safeguarding procedures are lacking
• Improper payments
• False or misleading information
• Pattern of large procurements in any budget line with remaining funds at year end
Risk Assessment (cont.)

• **Principle #9:** The organization identifies and assesses *changes* that could significantly impact the system of internal control.

• **Potential findings:**
  
  – Organization does not assess all types of *changes* that could impact the internal controls, i.e., changes in the external environment, the business model or leadership
Change

"You will be replacing Susan Johnson. To facilitate the transition, we’re having your name legally changed to Susan Johnson."
Component: Control Activities

• **Principle #10:** The organization selects and develops control activities that help mitigate risks to the achievement of objectives.

• **Potential findings:**
  – Control activities do not integrate with risk assessment
  – Control activities do not relate to business processes
  – Controls do not address segregation of duties
Control Activities (cont.)

- **Principle #11**: The organization selects and develops general control activities over **technology** to support the achievement of objectives.

- **Potential findings:**
  - Management does not establish relevant security management control activities
  - Management does not establish relevant technology acquisition, development and maintenance process control activities
Control Activities (cont.)

- **Principle #12:** The organization deploys control activities through **policies** that establish what is expected and **procedures** that put policies into action.

- **Potential findings:**
  - Missing or inadequate policies and procedures
  - Inadequate assignment of responsibility and accountability for executing policies and procedures
  - Failure to take corrective action on a timely basis.
  - Use of incompetent (unlicensed, untrained) personnel
Component: Information and Communication

• **Principle #13:** The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

• **Potential findings:**
  - Organization has failed to identify the information requirements to support functioning of internal controls (*Change orders? Cash forecasts?*)
  - Organization does not capture internal and external sources of data, and does not process data into relevant information (*Tax revenue forecasts?*)
**Information and Communication** (cont.)

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

- **Potential findings:**
  - Organization fails to communicate internal control information to *employees*
  - Organization fails to communicate internal control information with *management* or *Board*
Information and Communication (cont.)

• **Principle #15:** The organization **communicates with external parties** regarding matters affecting the functioning of internal control.

• **Potential findings:**
  – Does not communicate accurate information to external parties (grantors, bondholders, regulators)
  – Does not utilize relevant method of communication
Component: Monitoring Activities

• **Principle #16:** The organization selects, develops, and performs on-going and/or separate **evaluations** to ascertain whether the components of internal control are present and functioning.

• **Potential findings:**
  
  – Management does not integrate internal controls with business processes (*POs, approvals, contracting*)
  
  – Management fails to evaluate effectiveness of internal control on a regular basis (*self-assessment*)
Monitoring Activities (cont.)

- **Principle #17:** The organization evaluates and communicates internal control deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

- **Potential findings:**
  - Management fails to advise those responsible for correcting internal control deficiencies
  - Organization fails to require and monitor corrective action.
Objective #2 - Review

Objective - Understand internal control deficiencies that should lead to findings.

Summary – Each of the 17 Principles and 77 Points of Focus should be considered when assessing internal controls and identifying potential findings.
Objective #3 - Understand the key elements of an internal control finding
Internal Control Findings

© Randy Glasbergen
glasbergen.com

“The word ‘audit’ comes from ‘auditory’ which means ‘to hear bad news coming’.”
Elements of a Finding

Current Condition - What is the problem? Why is this an issue?

Criteria - What is the expected condition based on policy, law, best practice?

Cause - Why is there a difference between current condition and criteria? What is the ROOT cause?

Effect - What is the risk? What can happen if issues are not corrected?

Recommendation/Action Plan - What can be done to fix the root cause of a problem and improve processes?
Good vs Bad Control Language

Older Language ("Bad")
Quarterly, Controller reviews the AR allowance for adequacy and reasonableness of reserve amounts by initialing and dating the "AR reserve" analysis.

Updated Control ("Better")
• Quarterly, Controller reviews AR balances of significant customers with o/s balances greater than $10k and 5% of AR balance and those under the threshold by customer type (e.g. geographical location, types of orders, etc.), to review the AR allowance for accuracy and completeness. Final review of the AR reserve analysis is initialed and dated by the Controller which agrees to the final g/l balance for the period.
Condition

What is the problem? Why is this an issue?
“You embezzled 5 million dollars from the pension fund, you manipulated our stock with fraudulent accounting and took a box of pens home from the office. When you steal office supplies, it sets a bad example for everyone!”
Condition

Current Condition: Unit employees are not receiving the appropriate revenue training as required by Policy XXXX, Processing Revenue.

Sixteen of 25 (64%) employees reviewed did not have the appropriate revenue processing training and nine out of 19 (47%) employees reviewed did not have the appropriate Security Awareness Education (SAE) training.
Criteria

What is the expected condition based on policy, law, best practice?
Criteria

"The fine print, in the contract, can be read only if held up to a mirror."
Criteria

Policy XXX states, “Ensure all full time employees involved in revenue processing or with access to the Organization’s banking/payment card systems have attended a face to face Treasury revenue processing training session.”

Additionally, the policy states, “Attend ongoing training sessions delivered by Treasury; annual training is required for those involved with processing credit and debit card transactions.”
Why is there a difference between current condition and criteria?

What is the ROOT cause?
Cause – the Blame Factor

• Cause – may be willful disregard for policies/procedures or lack of knowledge of policies/procedures.
• Risk – the cause could reflect poorly on the auditee or appear as an excuse to the Board.
• Goal - must determine the ROOT cause of the issue to ensure the action plan will fix the problem.
Cause #1 – In response to recent budgetary constraints, staffing levels have decreased. Management overseeing the Unit expressed the opinion that staff did not have sufficient time to attend the training and also remain current with the processing of transactions.
Cause #2 – Management of the Revenue Processing Unit was not aware of the requirement for training. Further, communications in the form of newsletter notices, emails, posting to a calendar or other means were not utilized to help ensure awareness of upcoming training sessions.
Cause #3 – Management explained that staff had attended the training in the past and found it to be of limited value. They noted that the training materials had not been updated in at least five years.
Cause

Cause #4 – The required training is held only on the first Friday of every third month and, due to the Organization’s 9/80 work week, many employees are not on site to attend the training.
Effect

What is the risk?

What can happen if issues are not corrected?
Effect

Lack of appropriate training prior to processing revenue increases the risk for the loss of the organization’s funds.
Recommendation/Action Plan

What can be done to fix the root cause of a problem and improve processes?
Recommendation/Action Plan

Recommendation – We recommend management develop and implement a realistic timeframe by which all employees will complete the required Revenue training and/or the SAE training complete the training.
Recommendation/Action Plan

Recommendation (continued) – We further recommend management consult with Employee Development personnel regarding effective techniques to ensure awareness of upcoming training sessions.
Recommendation/Action Plan

Recommendation (continued) –
We recommend management advise Employee Development personnel of training needs based on such factors as Unit staff performance, new regulations or system changes.
Recommendation/Action Plan

Recommendation (continued) –
We recommend management work with Employee Development personnel regarding optimal dates for future training programs in order to facilitate attendance by all Unit staff.
Recommendation/Action Plan

**Action Plan** - All employees who have not taken the required Revenue training and/or the SAE training will complete the training by June 15, 2014.
Recommendation/Action Plan

Action Plan (expanded) - All employees who have not taken the required Revenue training and/or the SAE training will complete the training by June 15, 2014. Further, Unit management will meet with appropriate Employee Development personnel to resolve issues pertaining to notifications of training session, timing, and course content.
Objective #3 - Review

Objective - Understand the key elements of an internal control finding.

Summary – A complete finding should include **Condition, Criteria, Causes, Effect, and Recommendation/Action Plan.**
Objective #4 - Understand the process of evaluating and monitoring corrective action plans
Follow Up on Findings

• Consider relevancy of corrective action (address “root cause”).

• Validate stated corrective action.

• Consider summary table.
Corrective Action Plans
Collaboration between Internal Audit and the fiscal officer or involved management is key to implementing action plans.
Follow Up on Findings

**Status** - All employees who had not taken the required Revenue training completed the training by June 15, 2014. Further, Unit management has met with appropriate Employee Development personnel to resolve issues pertaining to notifications of upcoming training sessions, timing, and relevancy of content.
Objective #4 - Review

Objective - Understand the process of evaluating and monitoring corrective action plans.

Summary – Progress made in implementing corrective action plans should be monitored and reported, on a timely basis.
Objective #5 – Review the Top 10 Internal Control Findings
“Did you get any feedback on that audit report?”
Finding #10 – Lack of Inventory Controls

• **Current Condition** - Inventory controls don’t exist to control or monitor:
  – Shrinkage
  – Obsolete inventory
  – Accounting for inventory

• **Criteria** - Best Practice; GAAP; P&Ps

• **Risk** - Lost funds due to theft, spoilage, obsolescence
Finding #9 – Failure to Comply with Contracts or Agreements

- **Current Condition** – Lack of compliance with contracts, agreements, and memorandums of understanding
- **Criteria** - Provisions outlined in contract, agreements, memos
- **Risk** - Fines, penalties, reputation risk, legal risk for breach of contract
Finding #8 – Noncompliance with Purchasing Card Guidelines

• **Current Condition** - Purchasing cards used to:
  – Circumvent dollar limits by ‘stacking’ purchases
  – Purchase unallowable items
  – Purchase items which were available in-house

• **Criteria** - P-card process & restrictions

• **Risk** - Thousands of dollars could be spent before being detected because purchases are not pre-approved; theft.
Finding #7 — Lack of Procedures to Mitigate Risk

- **Current Condition** - Approved business processes not followed
- **Criteria** – P&Ps, Internal Controls; best business practice
- **Risk** - Undetected loss of funds, inefficiencies, theft.
Finding # 6 — Noncompliance with Policies & Related Laws

- **Current Condition** - Failure to have adequate internal controls to ensure policy compliance:
  - Delegation of signature authority
  - Lack of review/accountability
  - Fair Labor Standards Act
  - Conflict of Interest

- **Criteria** – P&Ps; Relevant Laws

- **Risk** - loss of funds; fines, penalties; reputation
Finding #5 - Noncompliance with Approved Revenue Processing Policies & Procedures

- **Current Condition** - Revenue policy is not followed with respect to:
  - Timely deposits
  - Credit card reconciliation
  - Endorsing checks

- **Criteria** - Processing Revenue Policy
- **Risk** - Theft, lost revenue, fines/penalties, reputational risk
Finding #4 – Failure to Pay Employees Accurately

• **Current Condition** - Employees pay not accurate
  – PTO adjustments for Absent without pay
  – Paid for not working (ghost employment)

• **Criteria** – Entity must pay only for time worked
  – Federal - FLSA, Effort Reporting (OMB A-87 and A-21)
  – State Law - Department of Labor
  – Organization’s policy

• **Risk** - Fines/penalties; disallowed grant costs; low employee morale; reputation
Finding #3 – Inadequate IT Physical Security

- **Current Condition** - Physical security inadequate.
- **Risk** - Loss of data, loss of equipment, harmed reputation, loss of funds.
Finding #2 – Inadequate IT Logical Security

- **Current Condition** - Policy regarding Security of IT Resources (software safeguards including user identification and password access, authenticating, access rights and authority levels) is not followed

- **Criteria** - Policy and best practices

- **Risk** - Security breach/lost data, lost dollars, reputational risk, legal issues
Finding #2 – Inadequate IT Logical Security: Examples

- Vulnerability scans
- Lack of disaster recovery plan/business continuity plan
- No review of system logs
- Backups
- Failing to encrypt data
- Anti-virus scans not performed
- Administrative rights
Finding # 1 – Failure to Secure Sensitive Data

• **Current Condition** - Sensitive data not secured (manual and electronic records)
• **Criteria** - guidance from Information Security & Privacy Program
• **Risk** - major fines, reputational risk, financial impact, personal liability, violations of state law.
Finding # 1 – Failure to Secure Sensitive Data: Examples

• HIPAA data
• PHI – protected health information
• Credit card numbers
• Check numbers
• SSN
Objective #5 - Review

Objective – Review the Top 10 internal control findings.

What Did We Learn

1. How to use the Framework to identify internal control deficiencies/findings
2. How to identify internal control deficiencies that should lead to findings
3. How to incorporate the key elements of an internal control finding
4. How to evaluate and monitor corrective action plans
5. The Top 10 Internal Control Findings
"Why couldn't my auditor have been someone like you?"
Contact Information

Peggy McBride

pmcbride@vasquezcpa.com

(213) 873-1706

(714) 231-6029