


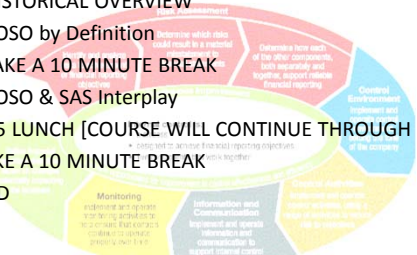
Internal Control and It's Impact on External Financial Reporting


Presented by
Steven L. Blake CPA, CFE, CICA, CGMA
 SLBCPA@CHARTER.NET 864-680-6191



Agenda

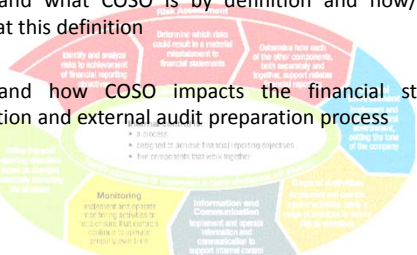
- 08:30 HISTORICAL OVERVIEW
- 09:15 COSO by Definition
- 10:00 TAKE A 10 MINUTE BREAK
- 11:30 COSO & SAS Interplay
- 12-12:15 LUNCH [COURSE WILL CONTINUE THROUGH LUNCH]
- 2:00 TAKE A 10 MINUTE BREAK
- 3:45 END



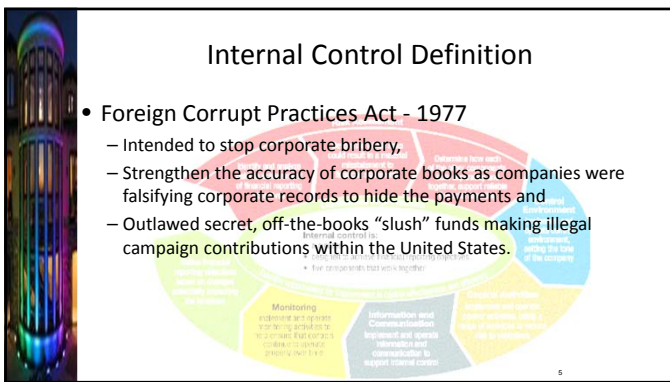


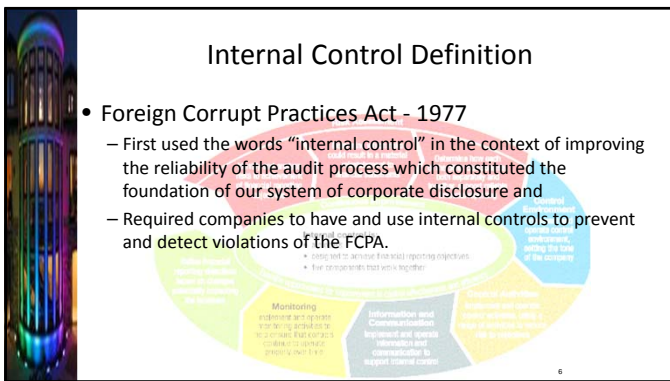
Learning Objectives

- Understand what COSO is by definition and how/why we arrived at this definition
- Understand how COSO impacts the financial statement preparation and external audit preparation process









Internal Control Definition

- There was a problem discovered early on in legal proceedings related to prosecution of FCPA violations: what is internal control?
- How much is enough?
- Who is responsible and at what level?

Internal Control Definition

- Hence the National Commission on Fraudulent Financial Reporting (the Treadway Commission) was formed in 1985
 - Original Chair, James C. Treadway, Jr. a Paine Webber attorney and former SEC Commissioner
 - Released a report on fraudulent financial reporting in October 1987
 - COSO was formed as a result of the report

Internal Control Definition

- COSO = the Committee of Sponsoring Organizations of the Treadway Commission
 - 5 Original Sponsors: AICPA, American Accounting Association [AAA], Financial Executives International [FEI], Institute of Internal Auditors [IIA] and Institute of Management Accountants [IMA]

Internal Control Definition

COSO is a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance.

Internal control is:
 • Integrated to achieve financial reporting objectives
 • Five components that work together

10

Internal Control Definition

- COSO produced its first framework in 1992
- Republished in 1994 with minor changes
- Reorganized in December 2011; expanded into principles and attributes; republished 2013
- COSO 2013 Framework effective 12-15-2014.

Internal control is:
 • Five components that work together

11

Internal Control Definition

- In a 2006 CFO magazine poll, 82% of respondents claimed they used COSO's framework for internal control.
- Other frameworks mentioned
 - SAS 55/78 (AICPA)
 - COBIT
 - PCAOB AS2

Internal control is:
 • Integrated to achieve financial reporting objectives
 • Five components that work together

12

Internal Control Definition

- In no legal way does COSO's framework apply to government or NGO's
- Sarbanes-Oxley does not apply either
- However, as we shall see later, COSO's framework is evaluated by anyone who is required to have a member of the AICPA audit their financial statements

Timeline

1987: Treadway Commission Report

1992: Internal Control - Integrated Framework

1996: Internal Control Issues in Derivatives

1999: Fraud Study I - Fraudulent Financial Reporting: 1987-1997

2004: Enterprise Risk Management Framework

2006: Guidance for Smaller Entities on Internal Control over Financial Reporting

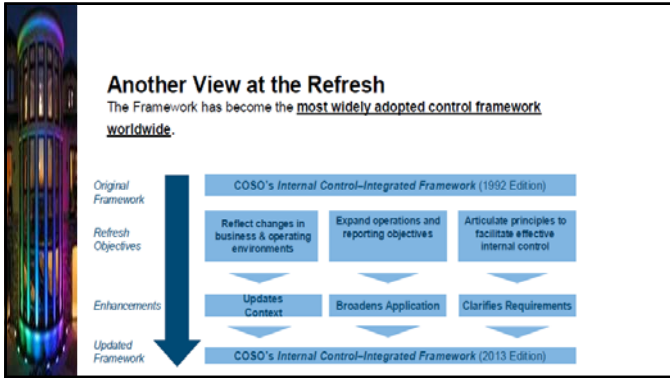
2009: Guidance on Monitoring Internal Control Systems

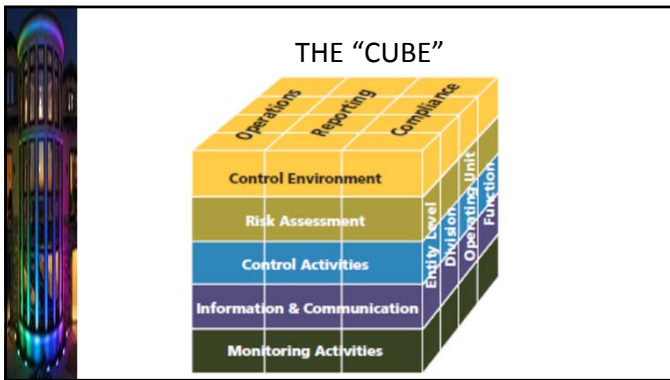
2010-2013: Recent ERM thought papers on current issues

2010: Fraud Study II - Fraudulent Financial Reporting: 1998-2007

COSO by Definition

- COSO by Definition
 - a process
 - designed to assure financial reporting objectives
 - four components that work together





Responsibilities and Objectives

- “...while effective internal control requires leadership from the top, the responsibility for effective implementation of internal control resides with everyone in the organization, not just the finance function. This includes accountants, compliance officers and those involved in making contracts and supporting operations as well as those working on the production line to ensure that products produced meet quality objectives.

...the individuals that are responsible for achieving the objectives are also responsible for the quality of internal controls.”

Larry Rittenberg
Chair Emeritus, COSO




Originally formed in 1985, COSO is a joint initiative of five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management (ERM) internal control and fraud deterrence.







> 600,000 members and global reach with all organizations




Mission

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."

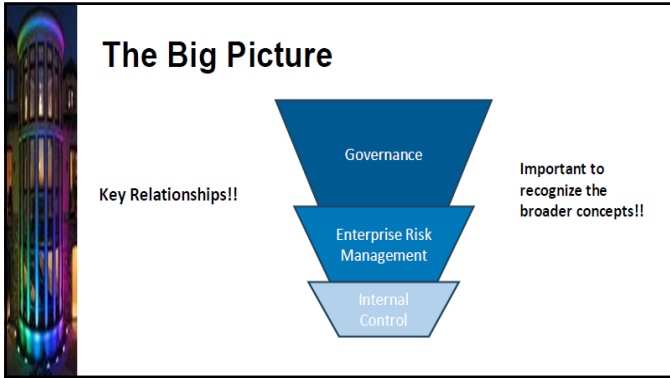
COSO's Fundamental Principle

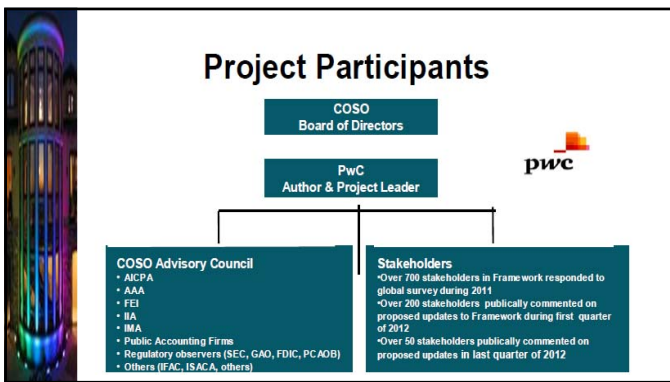
Good risk management and internal control are necessary for long term success of all organizations.

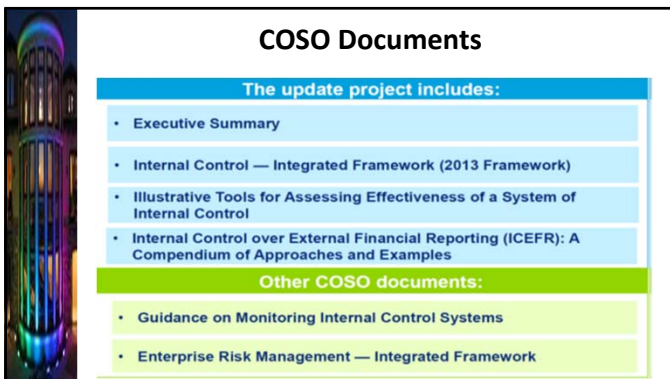


COSO releases new thought leader paper demonstrating how Frameworks improve organizational performance and governance

ALTAMONTE SPRINGS, Fla., Feb. 10, 2014: The Committee of Sponsoring Organizations of the Treadway Commission (COSO) announced today the release of a new thought paper, *Improving Organizational Performance and Governance: How the COSO Frameworks Can Help*, developed to illustrate how the enterprise risk management (ERM) and internal control frameworks can contribute to enhancing organizational performance and governance for sustainable success.







ERM and IC Framework Interaction

- From the Executive Summary of the 2-10-2014 Thought Paper:
 - “Within the context of its mission, an organization is designed to accomplish objectives.”

ERM and IC Framework Interaction

Risk Assessment in ICIF is Expanded into Three Components:
1) Event Identification 2) Risk Assessment and 3) Risk Response

ERM and IC Framework Interaction

Linking Organization Essentials

Who is responsible for each of these important elements?
Who determines the first four elements?
Are these part of internal control?

ERM and IC Framework Interaction

- From the Executive Summary of the 2-10-2014 Thought Paper:
 - “It is presumed that the organization’s leaders can articulate its objectives, [vision]
 - Develop strategies to achieve those objectives,
 - Identify the risks to achieving those objectives and
 - Mitigate those risks in delivering the strategy

Strategic View With an Enterprise Wide Approach

Use of the Framework in the context of

- Mission
- Vision
- Values
- Strategy


Entity level objectives: Operations, reporting (financial, non-financial, external, internal), compliance

ERM and IC Framework Interaction

Addresses Key Roles and Responsibilities

- Board of directors, board structure, board committees
- C-Suite
- Risk and control personnel
- Internal and external audit (of course!)
- Outsourced service providers
- Supply chain
- Legislators and regulators
- Analysts, bond rating agencies, news media, etc.


ERM and IC Framework Interaction



ERM Framework	COSO Framework
<ul style="list-style-type: none"> • Based on objective setting and • Identification of and • Mitigation or acceptance of risks to the achievement of those objectives 	<ul style="list-style-type: none"> • Designed to control risks to the achievement of objectives by reducing them to acceptable levels.


ERM and IC Framework Interaction

31

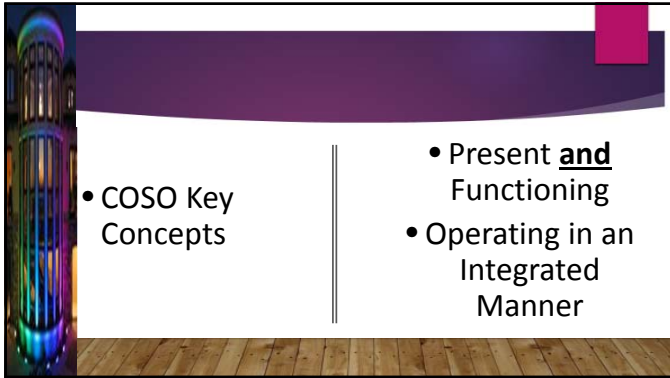


2013 Enhancements

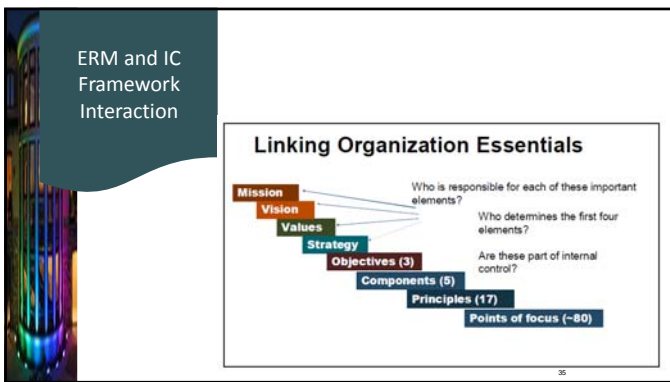
- Enhancements to:
 - Risk Assessment
 - More detailed discussions regarding risk concepts including inherent risk, risk tolerance, risk management and linking risk assessment to specific controls
 - Separately consider fraud risk related to objective achievement
 - Outside Service Providers
 - Specifically consider how they are monitored
 - Information Technology
 - How to include IT in continuous monitoring (Capability Maturity Model)
 - Requirements for ensuring data integrity/protection



Components	Principles
Control Environment	<ol style="list-style-type: none"> 1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	<ul style="list-style-type: none"> • Specifies suitable objectives • Identifies and analyzes risk • Assesses fraud risk • Identifies and analyzes significant change
Control Activities	<ul style="list-style-type: none"> • Selects and develops control activities • Selects and develops general controls over technology • Deploys through policies and procedures
Information & Communication	<ul style="list-style-type: none"> • Uses relevant information • Communicates internally • Communicates externally
Monitoring Activities	<ul style="list-style-type: none"> • Conducts ongoing and/or separate evaluations • Evaluates and communicates deficiencies

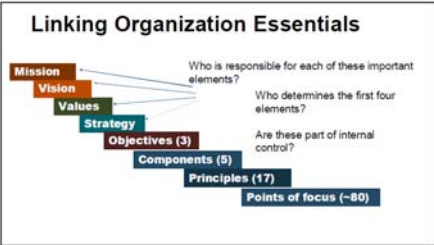


- COSO Key Concepts
- Present and Functioning
- Operating in an Integrated Manner



ERM and IC Framework Interaction

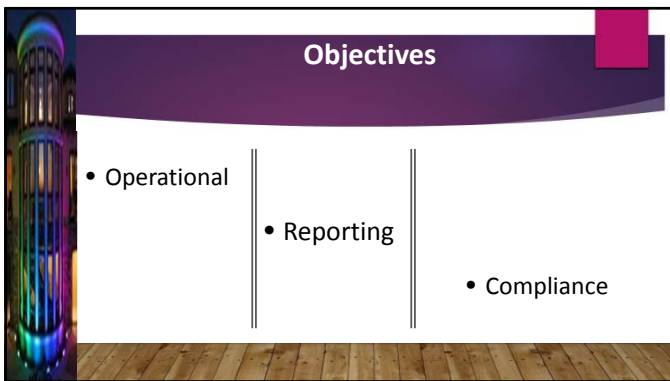
Linking Organization Essentials



Who is responsible for each of these important elements?

Who determines the first four elements?

Are these part of internal control?



Objectives

- Operational
- Reporting
- Compliance



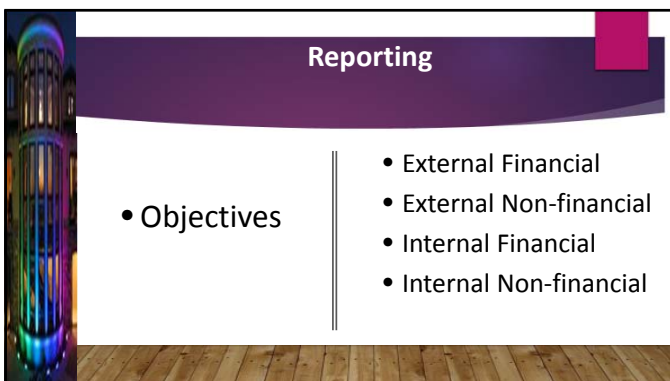
Operational

- Relate to the achievement of the basic mission and vision
- Spans financial performance, productivity, quality, environmental, innovation, customer service etc.



Operational

- Safeguard Assets
- Prevent loss
- Timely detect fraud
- Properly report loss
- Assess risk



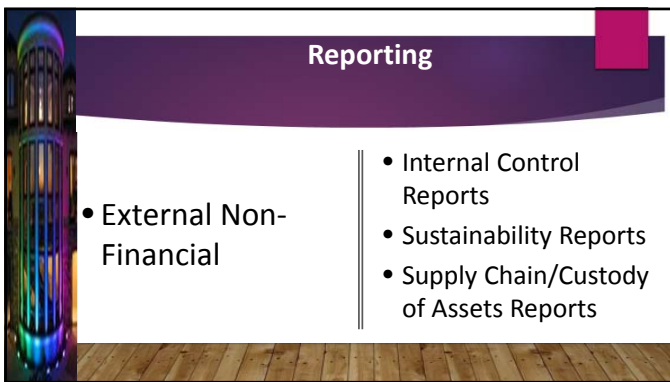
Reporting

- Objectives
- External Financial
- External Non-financial
- Internal Financial
- Internal Non-financial



Reporting

- External Financial
 - Annual Financial Statements
 - Interim Financials
 - Earnings Releases




Reporting

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




Reporting

- Internal Financial
 - Division Financials
 - Profitability Analysis
 - Bank Covenant Analysis




Reporting

- Internal Non-Financial
- Staff/Asset Utilization
- Customer Satisfaction
- Health & Safety



Compliance

- Understanding which laws & regs apply
- Incorporate minimum standards into objectives
- Determine if higher standards are necessary or desirable



Suitability & Relevance

- COSO views ALL five components as relevant & suitable to ALL entities.
- The 17 principles explain the components and, as such, are presumed relevant & suitable to ALL entities
- If a relevant principle is not present AND functioning, the associated component cannot be present & functioning.
 - In this rare instance, management is required to document how the component can be present & functioning when a principle is not.

AICPA Audit Standards

- In AU-C 315 regarding internal control and risk assessment, the standard defines internal control as: "A process effected by those charged with governance, management, and other personnel that is 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. Internal control over safeguarding of assets against unauthorized acquisition, use, or disposition may include controls relating to financial reporting and operations objectives. ¹

Objective of AU-C 315

- The objective **of the auditor** is to identify and assess the **risks of material misstatement**, whether due to **fraud** or **error**, at the **financial statement** and **relevant assertion levels** through understanding the entity and its environment, including the entity's internal control, thereby *providing a basis* for **designing** and **implementing responses** to the assessed risks of material misstatement.

AU-C Section 315

Division of internal control into components. The division of internal control into the following five components, for purposes of GAAS, provides a useful framework for auditors when considering how different aspects of an entity's internal control may affect the audit:

- The control environment
- The entity's risk assessment process
- The information system, including the related business processes relevant to financial reporting and communication
- Control activities
- Monitoring of controls



AU-C Section 315

- The **division** does not necessarily reflect how an entity designs, implements, and maintains internal control or how it may classify any particular component. Auditors may use different terminology or frameworks to describe the various aspects of internal control and their effect on the audit other than those used in this section, provided that all the components described in this section are addressed.



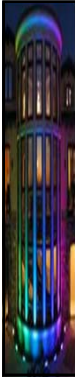
Auditor Risk Assessment Procedures

- Inquiries;
 - Of management
 - Individuals within the internal audit function, if applicable
 - Others who may have information
- Analytical Procedures
- Observation & Inspection



Understanding the Entity & It's Environment

- Industry, regulatory and other external factors
- Applicable financial reporting framework
- The nature of the entity:
 - Operations
 - Ownership/governance structure
 - Investment plans [resource investments to accomplish objectives]
 - Structure and financing
- Accounting policies and measurements and review of financial performance



Auditors' Understanding Limited

- Section 315, paragraph .13: The auditor should obtain an understanding of internal control **relevant to the audit**
- Likely the controls the auditor obtains an understanding of will relate to the financial reporting process, but not all process controls will be understood. Matter of professional judgment.



Nature & Extent of Understanding Relevant Controls

- The auditor should evaluate the design of those controls and determine whether they have been implemented by performing procedures *in addition to inquiry* of the entity's personnel
- The auditor should evaluate and document their understanding of internal control in each of the five component areas.



LUNCH TIME





Integration

- Each component cuts across and applies to all three categories of objectives.
- The three categories of objectives are not parts or units of the entity. For instance, operations objectives relate to the efficiency and effectiveness of operations, not specific operating units or functions such as sales, marketing, procurement, or human resources.



Objectives

- Management, with board oversight, sets entity-level objectives that align with the entity's mission, vision, and strategies.
- High-level objectives reflect choices made by management and board of directors about how the organization seeks to create, preserve, and realize value for its stakeholders.



Objectives

- May focus on the entity's unique operations needs, or align with laws, rules, regulations, and standards imposed by legislators, regulators, and standard setters, or some combination of the two.
- Objective setting is a ***prerequisite to internal control*** and a key part of the management process relating to strategic planning.



Objectives

- Individuals who are part of the system of internal control need to understand the overall strategies and objectives set by the organization.
- As part of internal control, management specifies suitable objectives so that risks to the achievement of such objectives can be identified and assessed.
- Specifying objectives includes the articulation of specific, measurable or observable, attainable, relevant, and time-bound objectives.



Objectives

- However there may be instances where an entity might not explicitly document an objective.
- Objectives specified in appropriate detail can be readily understood by the people who are working toward achieving them.



Operations Objectives

- relate to the achievement of an entity's basic mission and vision—the fundamental reason for its existence.
- vary based on management's choices relating to the management operating model, industry considerations, and performance
- Entity-level objectives cascade into related sub-objectives for operations within divisions, subsidiaries, operating units, and functions, directed at enhancing effectiveness and efficiency in moving the entity toward its ultimate goal



Operations Objectives

- may relate to improving financial performance, productivity (e.g., avoiding waste and rework), quality, environmental practices, innovation, and customer and employee satisfaction
- pertain to all types of entities
- if they are not well conceived or clearly specified, its resources may be misdirected



Operations Objectives

- Could include:
 - Safeguarding of Assets
 - efficient use of an entity's assets
 - prevention of loss through waste, inefficiency, or poor business decisions (e.g., selling product at too low a price, extending credit to bad risks, failing to retain key employees, allowing patent infringement to occur, incurring unforeseen liabilities)



Sub-objectives

- Management links specified entity-level objectives to more specific sub-objectives that cascade throughout the organization.
- Sub-objectives also are established as part of or flowing from the strategy-setting process, and relate to the entity and its subunits and functional activities such as sales, production, engineering, marketing, productivity, employee engagement, innovation, and information technology.
- Management aligns these sub-objectives with entity-level objectives and coordinates these across the entity.



Sub-objectives

- Where entity-level objectives are consistent with prior practice and performance, the linkage between activities is usually known.
- Where objectives depart from an entity's past practices, management addresses the linkages or accepts increased risks.



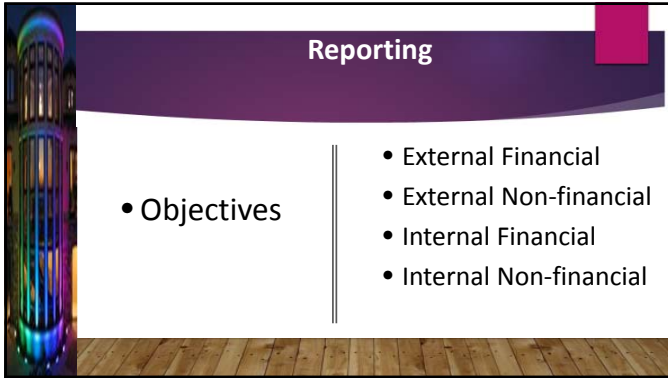
Sub-objectives

- Sub-objectives for operating units and functional activities also need to be specific, measurable or observable, attainable, relevant, and time-bound.
- In addition, they must be readily understood by the people who are working toward achieving them. Management and other personnel require a mutual understanding of both what is to be accomplished and the means of determining to what extent it is accomplished in order to **ensure individual and team accountability**



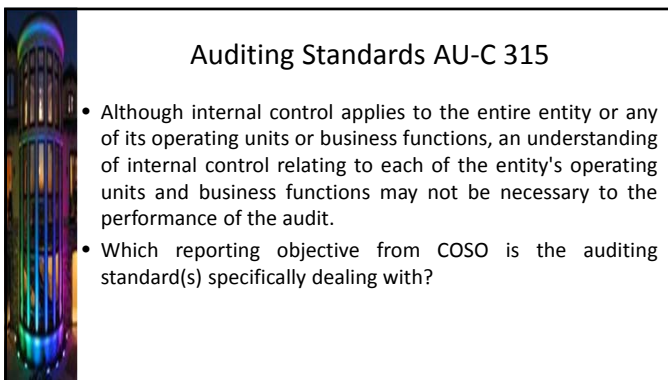
Reporting Objectives

- pertain to the preparation of reports that encompass
 - reliability,
 - timeliness,
 - transparency, or
 - other terms as set forth by regulators, standard-setting bodies, or by the entity's policies



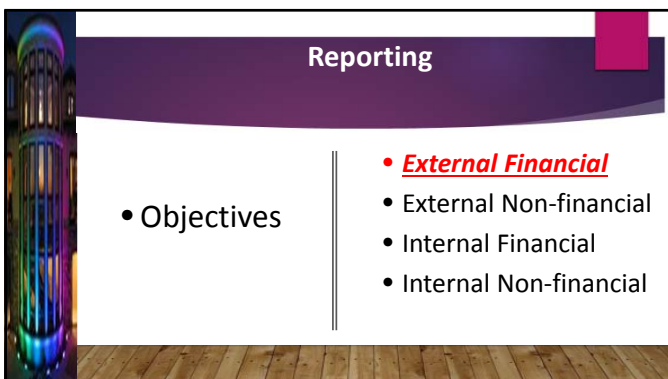
Reporting

- Objectives
 - External Financial
 - External Non-financial
 - Internal Financial
 - Internal Non-financial




Auditing Standards AU-C 315

- Although internal control applies to the entire entity or any of its operating units or business functions, an understanding of internal control relating to each of the entity's operating units and business functions may not be necessary to the performance of the audit.
- Which reporting objective from COSO is the auditing standard(s) specifically dealing with?




Reporting

- Objectives
 - ***External Financial***
 - External Non-financial
 - Internal Financial
 - Internal Non-financial




Auditor Risk Assessment Procedures

- Inquiries;
 - Of management
 - Individuals within the internal audit function, if applicable
 - Others who may have information
- Analytical Procedures
- Observation & Inspection



AU-C 315 Relevant Controls

- Factors relevant to the auditor's professional judgment about whether a control, **individually or in combination with others**, is **relevant to the audit** may include such matters as the following:
 - Materiality
 - The significance of the related risk
 - The size of the entity
 - The nature of the entity's business, including its organization and ownership characteristics



AU-C 315 Relevant Controls

- Factors relevant to the auditor's professional judgment about whether a control, **individually or in combination with others**, is **relevant to the audit** may include such matters as the following:
 - The diversity and complexity of the entity's operations
 - Applicable legal and regulatory requirements
 - The circumstances and the applicable component of internal control
 - The nature and complexity of the systems that are part of the entity's internal control, including the use of service organizations
 - **Whether and how** a **specific control**, individually or in combination with other controls, **prevents**, or **detects and corrects**, **material misstatements**

Objective of AU-C 315

- The objective of **of the auditor** is to identify and assess the **risks of material misstatement**, whether due to **fraud or error**, at the **financial statement** and **relevant assertion levels** through understanding the entity and its environment, including the entity's internal control, thereby *providing a basis* for **designing** and **implementing responses** to the assessed risks of material misstatement.

Assertions

- | | |
|--|--|
| <ul style="list-style-type: none"> • COSO • International focus & definition • Fundamental characteristics <ul style="list-style-type: none"> • Enhancing characteristics | <ul style="list-style-type: none"> • AU-C 315 • Relate to classes of transactions & events for the period • Relate to account balances at period end <ul style="list-style-type: none"> • Relate to presentation & disclosure |
|--|--|

COSO Fundamental Characteristics

- Relevance – makes a difference to the user
- Faithful Representation – information is complete, neutral and free from error



COSO Enhancing Characteristics

- Comparability – comparable with similar entities [across entities] or to the same entity as of another date [across time periods]
- Verifiability – different knowledgeable and independent observers reaching consensus, although not necessarily complete agreement that depiction is a faithful representation
- Timeliness – available to be used
- Understandability – classified, characterized & presented clearly and concisely



Transaction Assertions

- Occurrence – recorded ones occurred & relate to entity
- Completeness – events/trans. that should be, have been
- Accuracy – appropriate recording
- Cutoff – proper accounting period
- Classification – proper account



Account Balance Assertions

- Point in time – balance sheet date
- Existence – real, substantiated, exist
- Rights & obligations – entity specific, solely
- Completeness
- Valuation & allocation – appropriate amounts, including valuation adjustment accounts which coincide



Presentation & Disclosure Assertions

- Occurrence & rights and obligations: disclosed events, transactions and other matters occurred and pertain to entity
- Completeness – All necessary disclosures are included
- Classification & understandability – appropriately presented, described and clearly expressed
- Accuracy & valuation – disclosed fairly and in appropriate amounts



Assertions Specific to Governmental Entities

- transactions and events have been carried out in accordance with law or regulation.
- Such assertions may fall within the scope of the financial statement audit



Materiality

- COSO
 - Based on international standard language
 - Sets relevance threshold
 - Material IF omission or misstatement could influence decision-makers
 - Depends on size or circumstance of omission or misstatement
- AU-C 315
 - Reference AU-C 320
 - Misstatements, including omissions, are material if they individually or in the aggregate influence decision-makers
 - Judgements regarding it are made in light of circumstances and are affected by size or nature or both
 - Impact on groups, not individuals



AU-C 315 Relevance and IT

- The use of information systems [IT] or lack thereof, the capability maturity of IT, manual versus IT processes, all impact the relevance of controls for the audit.



Auditor Responses to Risk at the FS Level

- Emphasizing a higher degree of skepticism
- Assigning more experienced staff members, people with specialized skills [CISA] or specialists.
- Provide more supervision
- Incorporating unpredictability
- Changing up the nature, timing and extent of testing from year to year. IE higher the risk, more procedures at year end; less interim work



AU-C Risk Assessment Procedures at AL

- Should obtain evidence about the design & implementation and include:
 - DESIGN:
 - Inquiry
 - Observation of specific control
 - Inspect documents and reports
 - Tracing transactions through the system relevant to financial reporting [walk throughs]



AU-C Risk Assessment Procedures

- Should obtain evidence about the design & implementation and include:
 - IMPLEMENTATION:
 - If IT based control, it may suffice if observed at a given time, that it is implemented for the period when combined with the testing of controls over IT; in particular, IT program changes.
 - References AU-C 330 *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained* which requires:



AU-C 330

- IMPLEMENTATION:
- Perform a 'test of controls' regarding operating effectiveness of a particular control(s) at the assertion level by testing:
 - How the controls were applied at relevant times during the period
 - Consistency with which applied
 - By whom or what means including whether the person performing the control possesses the necessary authority and competence to perform effectively
 - Are the tested controls dependent on other controls?



AU-C 330

- IMPLEMENTATION:
- Relying on evidence obtained in previous audits:
 - Perform initial design procedures every year to inquire as to any changes from previous years' control(s) system. This is designed to establish 'continuing relevance'.
 - If there are changes, retest in the current year
 - Determine if a lack of change is warranted given the change in the entity from one year to the next
 - Determine how well the entity monitors and reports on the effectiveness of the control in the interim from year to year



AU-C 330

IMPLEMENTATION:

- Relying on evidence obtained in previous audits:
 - Test the controls, regardless, once every three years and should test them on a rotating basis so no one year has all control testing skipped.
 - HOWEVER, if this is a control over a ‘significant’ risk, it should be tested every year, regardless.



AU-C 330

- Other items of note:
 - Must test the “Financial Statement Closing Process” as its own separate process to be tested by
 - Comparing the financial statement with underlying accounting records
 - Journal entry testing, especially closing journal entries
 - Significant Risks need specific responses in the form of substantive procedures tied to that risk in the testing of details. In other words, document a link between the response and the risk.



Uniform Guidance Rules

- As COSO has a “Compliance” objective, so do federal grants
- Federal grant rules include external audit rules and these are found in the “Uniform Guidance” which all grantees are subject to since 12-31-15 audit year ends.
- Chapter 16 of this guidance requires the auditor to plan the internal control testing over compliance to support a low assessed level of control risk. IE larger sample sizes, more testing.

COSO Principles

- CONTROL ENVIRONMENT

1. Demonstrates a commitment to integrity and ethical values
2. Exercises oversight responsibility
3. Establishes structure, authority and responsibility
4. Demonstrates commitment to competence
5. Enforces accountability

COSO Principles

- RISK ASSESSMENT

6. Specifies suitable objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Identifies and analyzes significant change

COSO Principles

- CONTROL ACTIVITIES

10. Selects and develops control activities
11. Selects and develops general controls over technology
12. Deploys through policies and procedures

COSO Principles

- INFORMATION & COMMUNICATION
 - 13. Uses relevant information
 - 14. Communicates internally
 - 15. Communicates externally

COSO Principles

- MONITORING
 - 16. Conducts ongoing and/or separate evaluations
 - 17. Evaluates and communicates deficiencies

