Powerful Insights.
Proven Delivery.®

COSO 2013

What's New, What's Changed, Why Does it Matter and Other Frequently Asked Questions

protiviti®
Risk & Business Consulting.
Internal Audit.

Today's Presenter

Jonathan Reiss is a Director in Protiviti's New York office in the Internal Audit Practice. He has over 13 years' experience (11 years with Protiviti) working with companies across multiple industries in the areas of Internal Audit, Sarbanes Oxley and Financial and Operation Controls. Jonathan works closely with Internal Audit Directors, CFOs and Controllers in accomplishing their objectives and facilitates the delivery of Protiviti's services related to Internal Audit and Financial Controls.

Jonathan.Reiss@protiviti.com

protiviti®

Today We Will Cover

- Background on COSO
- Why Change?
- Important Changes
- Deficiency Evaluation
- Transitioning to the New Framework

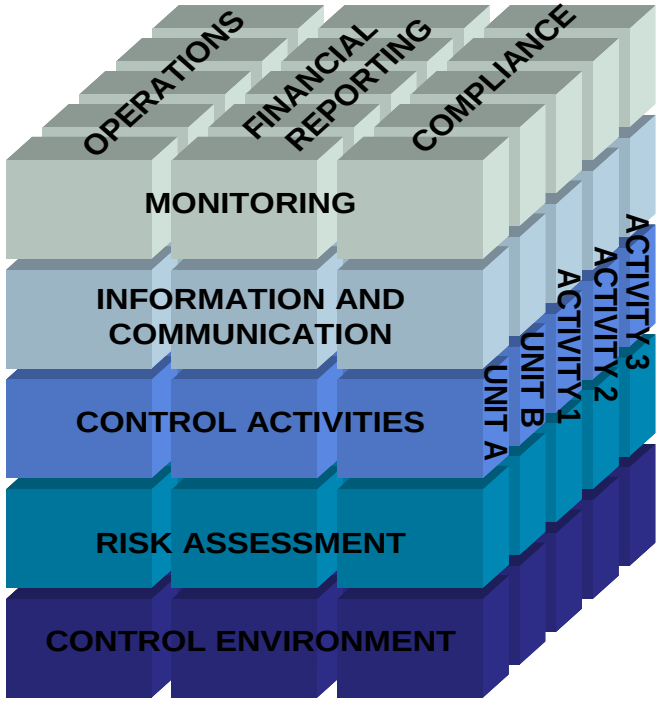
protiviti®

Why Change?

Background and History of COSO

Committee Of Sponsoring Organizations of the Treadway Commission

- Formed in 1985 in response to corrupt and unethical business practices in the 1970's and 80's
- Voluntary private sector organization
- COSO Internal Control Integrated Framework was developed in 1992
- Used by the majority of companies to evaluate their internal control environment, particularly as it relates to internal controls over financial reporting



COSO Cube (1992 Edition)

SPONSORING ORGANIZATIONS

AICPA fei IIA IMA

protiviti

What is COSO and Why is it a Suitable Model?

Management is required to base its assessment of the effectiveness of the company's internal control over financial reporting on a ***suitable, recognized control framework*** established by a ***body of experts that followed due-process procedures, including the broad distribution*** of the framework for public comment.

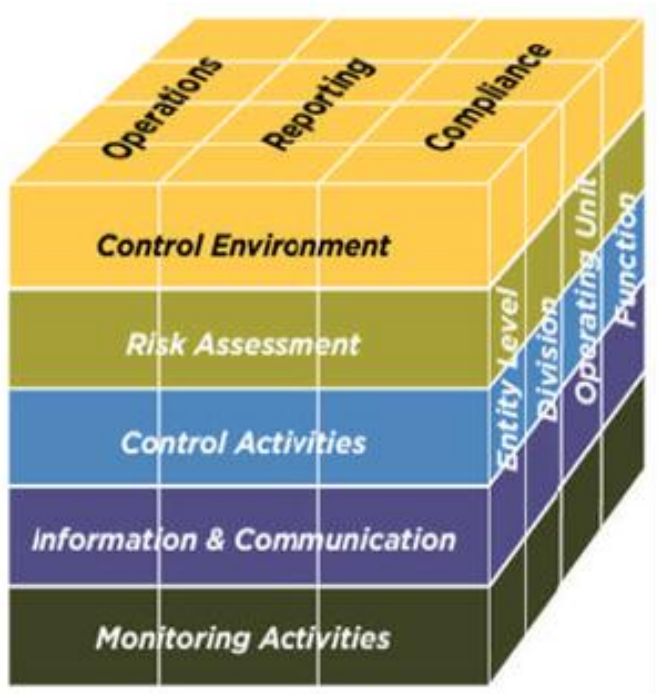
Source: PCAOB AS2

Why Change?

Environment changes…

- Expectations for governance oversight
- Risk and risk-based approaches receive greater attention
- Globalization of markets and operations
- Increased complexity of business and organizational structures
- Use of, and reliance on, evolving technologies
- Demands and complexity in laws, rules, regulations and standards
- Large-scale governance and internal control breakdowns
- Expectations for competencies and accountabilities
- Expectations relating to preventing and detecting fraud

…have driven Framework updates



COSO Cube (2013 Edition)*

* **Source:** Chapter 2 of COSO *Internal Control: Integrated Framework (2013)*.

protiviti®

What Hasn't Changed

Core definition of internal control

Internal control is a process effected by the entity's board of directors, management and other personnel designed to provide reasonable assurance regarding the achievement of objectives relating to:

Operations **Reporting** **Compliance**

The cube retains its familiarity:

- Objectives represent the columns
- Components represent the rows
- Objectives may be set at the entity, division, operating unit or functional levels

protiviti®

What Hasn't Changed

The criteria used to assess the effectiveness of an internal control system remain largely unchanged.

Assessed, using a principles-based approach, relative to the five components of internal control

To have an effective system of internal control relating to one, two or more categories of objectives, all five components must be:

- *Present and functioning*, and
- Operating together

The significant role of judgment in designing, implementing and conducting internal control, and in assessing its effectiveness.

Principles are provided for each component and management exercises judgment in determining the extent to which these principles are *present and functioning*

protiviti®

What's Changed

1. Codifies 17 principles supporting the five components of internal control
2. Clarifies role of objective-settling as a precursor to internal control
3. Reflects increased relevance of technology
4. Incorporates an enhanced discussion of governance concepts
5. Expands the reporting category of objectives to include non-financial and internal
6. Enhances consideration of anti-fraud expectations in its own principle
7. Increases the focus on non-financial reporting objectives to broaden use
8. Additional approaches and examples for operations, compliance and non-financial reporting objectives

protiviti®

Important Changes

The Most Important Change: 17 Principles Representing Fundamental Concepts Associated with Each Component

		No of POF Questions
CONTROL ENVIRONMENT	• Demonstrates commitment to integrity and ethical values	4
	• Exercises oversight responsibility	4
	• Establishes structure, authority and responsibility	3
	• Demonstrates commitment to competence	4
	• Enforces accountability	5
RISK ASSESSMENT	• Specifies relevant objectives	5
	• Identifies and analyzes risk	5
	• Assesses fraud risk	4
	• Identifies and analyzes significant change	3
CONTROL ACTIVITIES	• Selects and develops control activities	6
	• Selects and develops general controls over technology	4
	• Deploys through policies and procedures	6
INFORMATION & COMMUNICATION	• Uses relevant information	5
	• Communicates internally	4
	• Communicates externally	5
MONITORING ACTIVITIES	• Conducts ongoing and/or separate evaluations	7
	• Evaluates and communicates deficiencies	3

protiviti®

Points of Focus Represent Important Characteristics Associated With the Principles

Principles can be present and functioning without all points of focus. Points of focus represent helpful guidance and do not require separate evaluations. Management must use judgment on the relevance of the points of focus. They are not meant to imply a checklist. An example of these for the Control Environment, Commitment to Integrity and Ethical Values is below.

Sets the Tone at the Top

The board of directors and management at all levels of the entity demonstrate through their directives, actions and behaviors the importance of integrity and ethical values to support the functioning of the system of internal control

Establishes Standards of Conduct

The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the organization and by outsourced service providers and business partners

Evaluates Adherence to Standards of Conduct

Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct

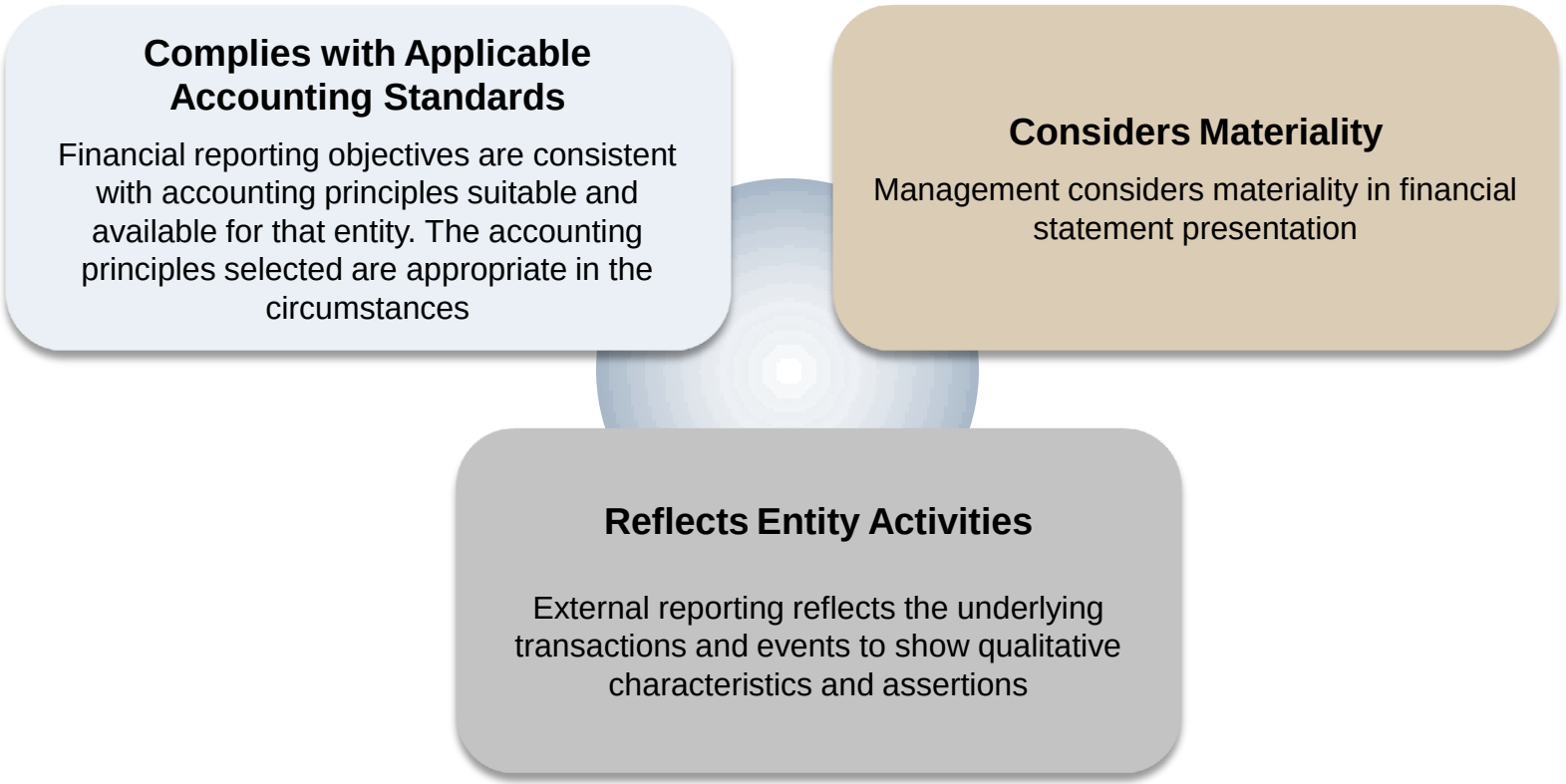
Addresses Deviations in a Timely Manner

Deviations from the entity's expected standards of conduct are identified and remedied in a timely and consistent manner

protiviti®

Practical Application – Points of Focus: Important Characteristics

An example of these for Risk Assessment - Specifies Relevant Objectives - is below.



protiviti®

Practical Application – Points of Focus: Important Characteristics

An example of these for Control Activities - Selects and Develops Control Activities - is below.

Integrates with Risk Assessment

Control activities help ensure that risk responses that address and mitigate risks are carried out

Considers Entity-Specific Factors

Management considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities

Determines Relevant Business Processes

Management determines which relevant business processes require control activities

Evaluates a Mix of Control Activity Types

Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls

Considers at What Level Activities Are Applied

Management considers control activities at various levels in the entity

Addresses Segregation of Duties

Management segregates incompatible duties, and where such segregation is not practical, selects and develops alternative control activities

protiviti®

Practical Application – Points of Focus: Important Characteristics

An example of these for Information and Communication - Uses Relevant Information - is below.

Identifies Information Requirements

A process is in place to identify the information required and expected to support the functioning of the other components of internal control and the achievement of entity's objectives

Captures Internal and External Sources of Data

Information systems capture internal and external sources of data

Processes Relevant Data into Information

Information systems process and transform relevant data into information

Maintains Quality throughout Processing

Information systems produce information that is timely, current, accurate, complete, accessible, protected, and verifiable and retained. Information is reviewed to assess its relevance in supporting the internal control components

Considers Costs and Benefits

Management considers control activities at various levels in the entity

protiviti®

Practical Application – Points of Focus: Important Characteristics

An example of these for Monitoring Activities - Conducts Ongoing and/or Separate Evaluations - is below.

Considers a Mix of Ongoing and Separate Evaluations

Management includes a balance of ongoing and separate evaluations

Considers Rate of Change

Management considers the rate of change in business and business processes when selecting and developing ongoing and separate evaluations

Establishes Baseline Understanding

The design and current state of an internal control system are used to establish a baseline for ongoing and separate evaluations

Uses Knowledgeable Personnel

Evaluators who perform ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated

Integrates with Business Processes

Ongoing evaluations are built into the business processes and adjust to changing conditions

Adjusts Scope and Frequency

Management varies the scope and frequency of separate evaluations depending on risk

Objectively Evaluates

Separate evaluations are performed periodically to provide objective feedback

protiviti®

Deficiency Evaluation

Present and Functioning

To determine that a principle and component are "present and functioning", the organization must:

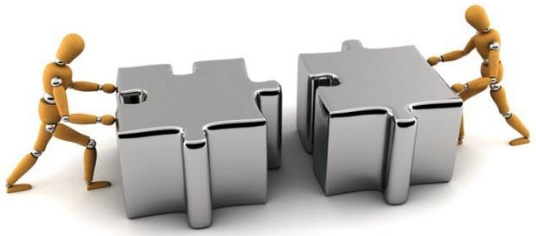
- Understand the intent of the principle and how it is being applied
- Work to help personnel understand and apply the principle consistently across the entity
- View weaknesses in absence of a principle as a matter requiring management's attention

- ***"Present"*** refers to "the determination that components and relevant principles exist in the design and implementation of the system of internal control to achieve specified objectives" (Design and Implementation Effectiveness)
- ***"Functioning"*** refers to "the determination that components and relevant principles continue to exist in the conduct of the system of internal control to achieve specified objectives" (Operating Effectiveness)
- Determine to what extent relevant principles underlying the component are "present and functioning"

protiviti®

Assessing Whether Components Operate Together

- **Focus of evaluation** is on how each of the five components is being applied as an integral part of the overall system of internal control, not just functioning on its own
- Components **are interdependent** with a multitude of interrelationships and linkages, particularly in terms of how principles interact within and across components
- From a practical standpoint, **management can demonstrate** that components operate together when they are present and functioning AND internal control deficiencies aggregated across components do not result in the determination that one or more major deficiencies exist
- Therefore, **aggregate** internal control deficiencies across components to assess whether major deficiencies exist



Assessment of Internal Control Deficiencies

A deficiency is “a short-coming in a component or components and relevant principle(s) that reduces the likelihood that the entity can achieve its objectives.” Not every deficiency will result in a conclusion that the entity does not have an effective system of internal control.

- **Major deficiency =** “an internal control deficiency or combination of deficiencies that severely reduces the likelihood that the entity can achieve its objectives”
- Management **may be required** to consider additional criteria established by external parties (e.g., regulators, standard-setting bodies, listing agencies, etc.)
- Alternative or compensating controls **may further support** a conclusion that a principle is present and functioning

protiviti®

Limitations on Internal Control

- No such thing as absolute assurance
- The framework comments on limitations of internal control, which results from:
  - The quality and suitability of objectives established as a precondition to internal control
  - The potential for flawed human judgment in decision-making
  - Management's consideration of the relative costs and benefits in responding to risk and establishing controls
  - The potential for breakdowns that can occur because of human failures (such as simple errors or mistakes)
  - The possibility that controls can be circumvented by collusion of two or more people
  - The ability of management to override internal control functions and decisions

Transitioning to the New Framework

Illustrative High Level Project Plan – Gap Analysis Example

Inventory existing key controls and evaluate to see if all principles are present and functioning. Determine appropriate points of focus to evaluate against.

Gap Analysis		Principle																
			Control Environment					Risk Assessment				Control Activities			Information and Communication			Monitoring Activities
Primary Control #	Control description	Demonstrates commitment to integrity and ethical values	Exercises oversight responsibility	Establishes structure, authority and responsibility	Demonstrates commitment to competence	Enforces accountability	Specifies suitable objectives	identifies and analyzes risks	Assesses fraud risk	Identifies and analyzes significant changes	Selects and develops control activities	Selects and develops general control over technology	Deploys through policies and procedures	Uses relevant information	Communicates internally	Communicates externally	Conducts ongoing and/or separate evaluations	Evaluate and communicates deficiencies
1	Entry level control 1	x	x	x	x			x							x	x		
2	Entry level control 2	x	x	x	x			x	x	x					x	x	x	
	...				x	x			x		x	x		x	x	x	x	
	...				x	x		x	x	x	x	x		x	x		x	
102	Close the books-Reconciliation A				x	x		x		x	x	x		x	x	x	x	
103	Close the books mgmt review				x	x			x	x	x			x	x	x	x	
104	Etc..					x			x	x		x		x	x	x	x	
	Principle Present and Functioning	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No

protiviti®

Get External Auditor Involvement Upfront

Orientation | **Planning** | Assessment | Remediation

- Meet with **external auditor** to discuss expectations
  - Get their views on approach and issues
  - Determine their expectations on changes in documentation
  - Understand the key changes they see related to the company's previous approach
  - Align approach where appropriate to drive efficiencies and support reliance upon your work
  - Identify areas that could be more difficult and require attention to address specific challenges

protiviti®

Preliminary Mapping Exercise for 17 Principles

- Determine the **mapping approach using the 17 principles**
- Identify the **relevant points of focus** for each principle
- Create 17 principles documentation inventory
  - Create document that lays out the 17 principles – under each principle summarize at a high level "what the company has that demonstrates this principle is present and functioning"
  - Come to an initial conclusion
    - we have it nailed
    - we are in pretty good shape with some refinements needed
    - we have some controls that are relevant but have work to do to complete, or
    - we must start from scratch
  - Use this perspective to plan the detailed mapping exercise

protiviti®

Mapping Controls to the 17 Principles - *Sample Scenarios*

COSO Component	Control Environment
Principle	1. The organization demonstrates a commitment to integrity and ethical values
Point of Focus	2. Establishes Standards of Conduct
Control Objective	A code of conduct and other policies exist regarding acceptable business practice, conflicts of interest, or expected standards of ethical and moral behavior and are effectively implemented within the organization.
Control Examples	The company has an employee handbook which contains the company's policies and change order procedures regarding: 1. Internet 2. Discrimination 3. Harassment 4. Health and Safety 5. Whistleblower 6. Code of Conduct and Business Ethics The policy includes guidelines for handling high risk matters and high risk geographies. It encourages personnel raise issues or questions related to the application of defined standards. It outlines explicit consequences for deviations.

protiviti®

Mapping Controls to the 17 Principles - *Sample Scenarios*

COSO Component	Control Environment
Principle 1, POF 2	The organization demonstrates a commitment to integrity and ethical values - Establishes Standards of Conduct (Code of Conduct cont'd)
Control Examples (cont'd)	The employee handbook is provided to all employees, when they are hired or when new versions come out. All employees must sign an acknowledgement that he/she has read the employee handbook. The signed acknowledgement of employee's understanding of, and compliance with the employee handbook is retained and filed in the employee's HR file.
	In the event of updates to the employee handbook, all employees are provided with an updated hardcopy or electronic copy (i.e., email or company's intranet). Additionally, each employee is required to read the updated policy, and to sign an acknowledgement. HR tracks the employees' acknowledgments and sends them a reminder.
	A supplier code of conduct is incorporated into supplier contracts.
	Ethics training is provided annually to staff in the finance function.

Mapping Controls to the 17 Principles - *Sample Scenarios*

COSO Component	Control Environment
Principle	1. The organization demonstrates a commitment to integrity and ethical values
Point of Focus	2. Establishes Standards of Conduct
Control Objective	An Insider Trading Policy is in place that details the Company's policy regarding trading in company shares are defined and the "covered person" and the other eligibility requirements.
Control Examples	An Insider Trading Policy Statement details the Company's policy regarding trading in company shares. "Covered Persons" are required to comply with the policy. At the time an employee is determined to be a covered person, they are provided a copy of the policy and must sign, acknowledging they understand the policy. Signed acknowledgements are retained by the company as evidence.

Assessment Phase

- **Map controls to principles** and come to a **preliminary conclusion** regarding whether
  1. the design of the documented controls is effective and
  2. if the controls are determined to be operating effectively, would they allow management to conclude that the Principle is “present and functioning”
- **Diagnose gaps** in documentation
- Determine controls that must be re-configured, changed, added/deleted for 2014, if any, to support a positive assertion in the internal control report
- Based on the above, finalize the action plan for 2014 to
  - improve the control structure
  - test the operating effectiveness of controls
  - arrange for the necessary resources
- **Meet with the external audit firm** and present results of work, identified areas for revision, remaining action plan, etc.

protiviti®

Assessment Phase – Opportunity to Assess Existing Controls

Orientation | Planning | **Assessment** | Remediation

- Assessment provides an opportunity to evaluate effective compliance with COSO. **Take the time to re-assess** your controls against the base COSO elements you have had in place for several years.
- Document controls that exist but were not previously documented and tested for SOX.

protiviti®

Assessment Phase – Points of Focus

Orientation | Planning | **Assessment** | Remediation

- Points of focus help drive the 17 principles to a more granular, actionable level
- While not required, they should be **used as a guideline** to assess conformance to the principles

protiviti®

Remediation

Orientation | Planning | Assessment | **Remediation**

- Execute remaining steps in the action plan and **monitor progress** to completion

protiviti®

Questions

protiviti®

Powerful Insights.
Proven Delivery.®