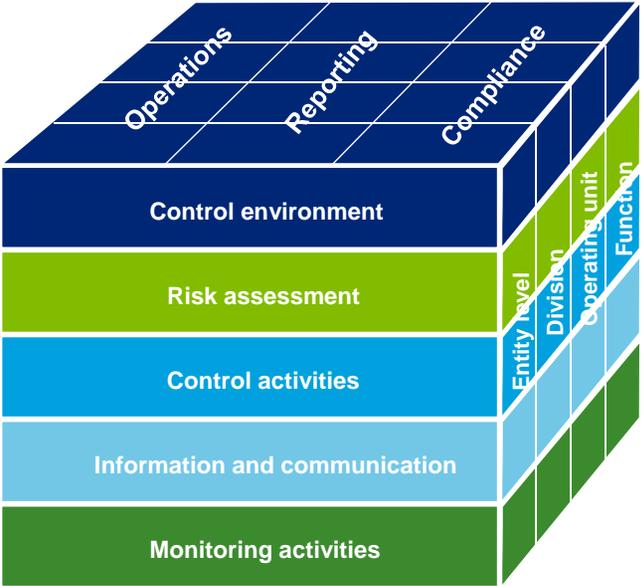




# 2013 COSO Framework – Overview and Considerations

June 2014



Official Professional Services Sponsor

Professional Services means audit, tax, consulting and financial advisory services.

# Contents

Introduction

Committee of Sponsoring Organizations of the Treadway Commission (COSO) guidance and framework overview

Internal control over financial reporting (ICFR): areas of focus and marketplace observations

Considerations and next steps

Resources

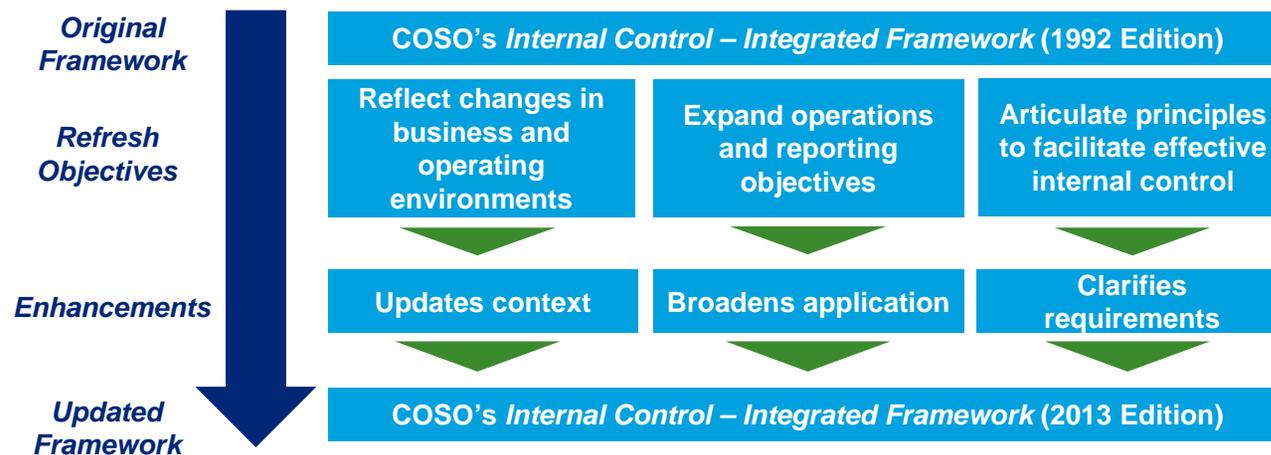
# Introduction

- A recent confluence of events has elevated the focus on internal controls
- With the release of the 2013 COSO Framework, entities have an opportunity to reassess the effectiveness and efficiency of their internal controls related to reporting, operations, and compliance objectives
- Entities should consider the value that can be created and the costs that can be avoided in the following areas:

Reporting	Operations	Compliance
<p>Objectively evaluate the entity's internal controls over financial reporting to:</p> <ul style="list-style-type: none"> <li>• Improve internal control in financial reporting</li> <li>• Avoid the adverse effects of costly material weaknesses or frauds</li> <li>• Reduce regulatory risk resulting from an increased focus on internal controls by Securities &amp; Exchange Commission (SEC) and Public Company Accounting Oversight Board (PCAOB)</li> <li>• Enhance external auditors ability to use management 's assessment as audit evidence</li> </ul>	<p>Leverage the COSO Framework to:</p> <ul style="list-style-type: none"> <li>• Provide helpful and necessary discipline to address the increasingly complex array of operational risks that boards oversee</li> <li>• Provide management with a consistent and efficient framework to define, implement, and monitor the control structure to:               <ul style="list-style-type: none"> <li>• Improve financial performance</li> <li>• Address cyber-security risks</li> <li>• Increase productivity and innovation</li> <li>• Improve quality</li> <li>• Improve customer and employee satisfaction</li> </ul> </li> <li>• Create governance, risk, and controls programs related to environmental practices and sustainability</li> </ul>	<p>Leverage the COSO Framework to manage compliance with:</p> <ul style="list-style-type: none"> <li>• Foreign Corrupt Practices Act</li> <li>• Managing compliance with global security and privacy regulations</li> <li>• Manage compliance with third-party contract agreements, including those related to security access and licensing requirements.</li> <li>• Focus on industry specific regulatory requirements</li> </ul>

# Highlights of the 2013 COSO Framework

COSO released an updated edition of *Internal Control – Integrated Framework* in 2013 (the “2013 COSO Framework”) to address changes in business and operating environments since the original framework’s release in 1992.



Globalization of markets and operations, complexities in laws and regulations, and the use and reliance on evolving technologies were factors in driving COSO to update the framework.

## The fundamental aspects of *Internal Control – Integrated Framework* have been retained:

- Core definition of internal control
- Three categories of objectives and five components of internal control
- Important role of judgment in designing, implementing, and conducting internal control, and in assessing its effectiveness

## Key changes include:

- More formal structure for the design and evaluation of the effectiveness of internal control
  - Establishes **principles** for each component of internal control
  - Provides **points of focus** regarding each **principle**
- Adds and refreshes guidance within each of the components of internal control

# Internal control components and associated principles

The 2013 COSO Framework addresses some of the key changes in the business environment since the original framework was published in 1992. The updated framework includes 17 principles to describe the components of internal control.

Control environment	Risk assessment	Control activities	Information and communication	Monitoring activities
<ol style="list-style-type: none"> <li>1. Demonstrates commitment to integrity and ethical values</li> <li>2. Exercises oversight responsibilities</li> <li>3. Establishes structure, authority, and responsibility</li> <li>4. Demonstrates commitment to competence</li> <li>5. Enforces accountability</li> </ol>	<ol style="list-style-type: none"> <li>6. Specifies suitable objectives</li> <li>7. Identifies and analyzes risk</li> <li>8. Assesses fraud risk</li> <li>9. Identifies and analyzes significant change</li> </ol>	<ol style="list-style-type: none"> <li>10. Selects and develops control activities</li> <li>11. Selects and develops general controls over technology</li> <li>12. Deploys through policies and procedures</li> </ol>	<ol style="list-style-type: none"> <li>13. Uses relevant, quality information</li> <li>14. Communicates internally</li> <li>15. Communicates externally</li> </ol>	<ol style="list-style-type: none"> <li>16. Conducts ongoing and/or separate evaluations</li> <li>17. Evaluates and communicates deficiencies</li> </ol>

**Per COSO, an effective system of internal control requires:**

- Each of the 17 principles to be present and functioning
- The five components of internal control to be present and functioning
- The five components to be operating together in an integrated manner

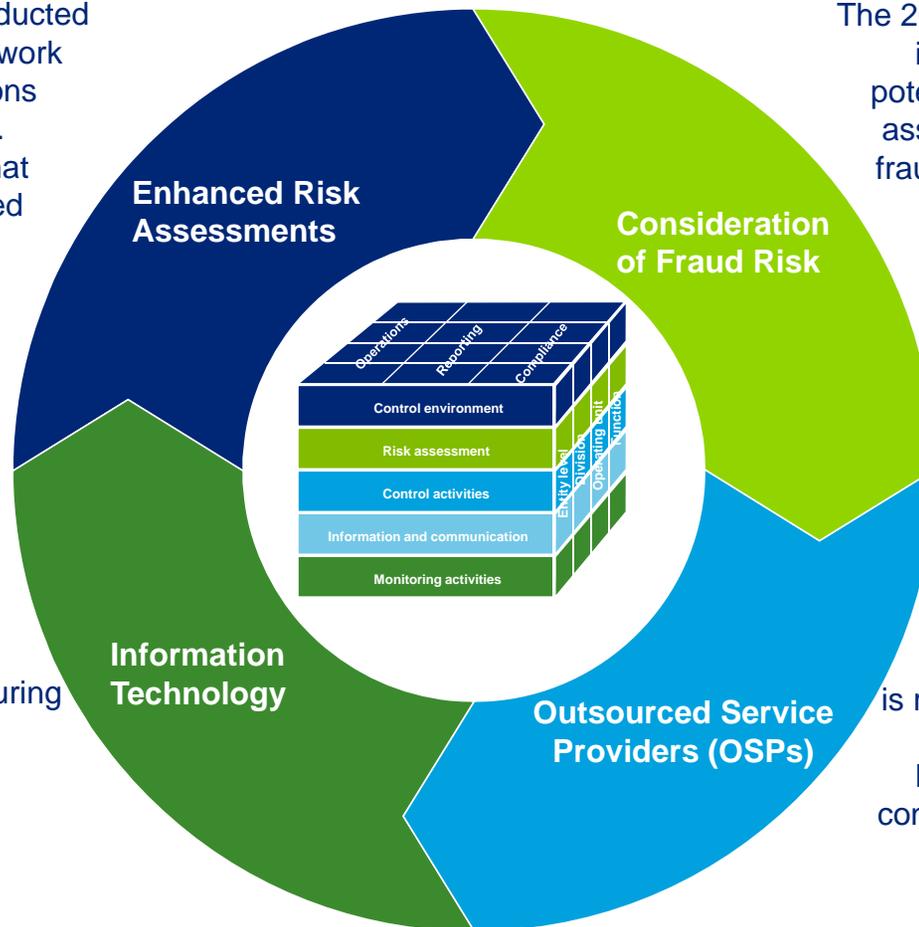
# Significant changes in the 2013 COSO Framework

## Enhanced Risk Assessments

Risk assessments are often conducted in silos. The 2013 COSO Framework provides more detailed discussions about risk assessment concepts. Entities should seek to ensure that they have a defined and approved risk assessment methodology that considers the 17 Principles.

## Information Technology

Entities with multiple lines of businesses, often operate fragmented IT systems. The 2013 COSO Framework includes additional considerations related to IT and provides considerations for ensuring the quality of information.



## Fraud Risk Assessments

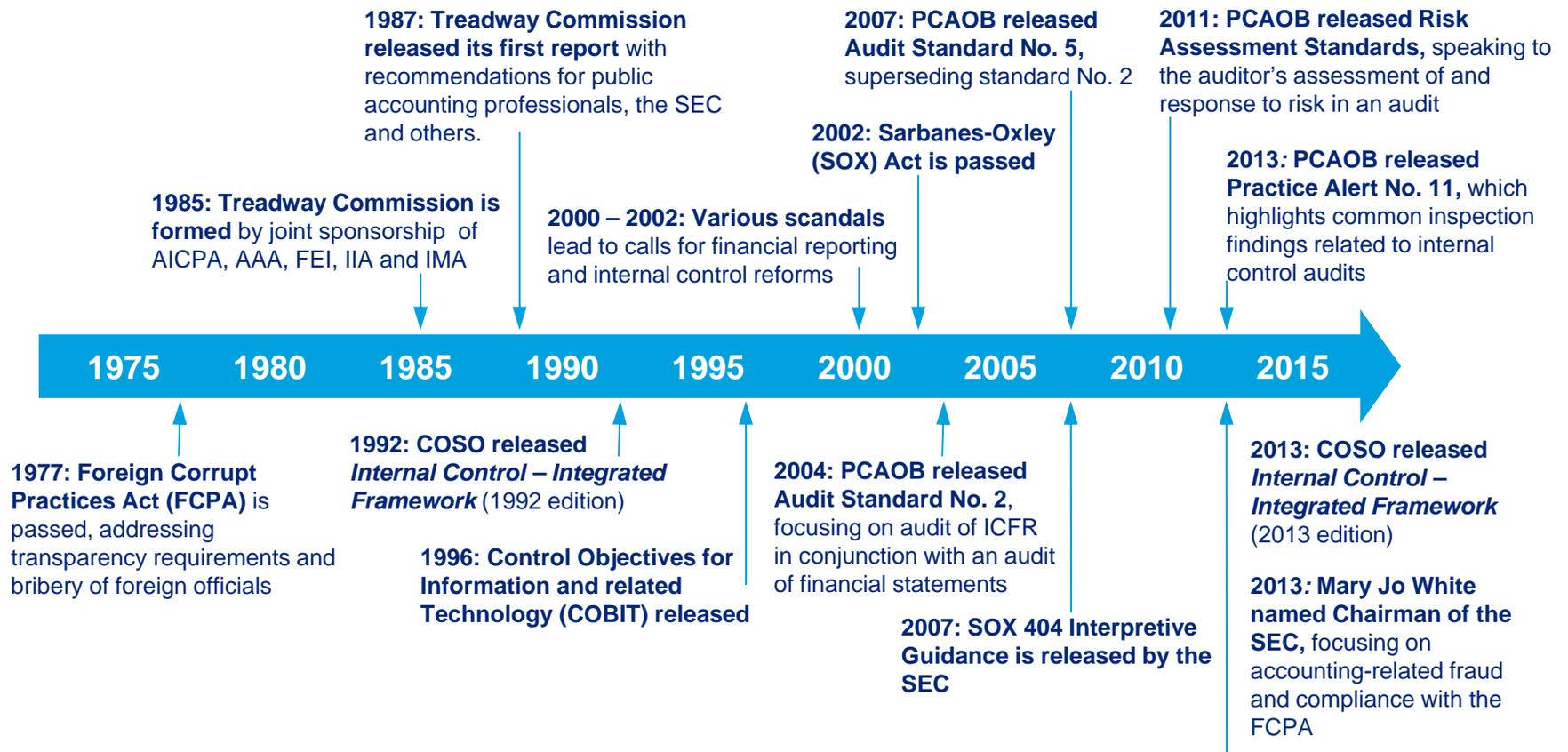
The 2013 COSO Framework explicitly includes the consideration of the potential for fraud in performing risk assessments. As part of assessing fraud risks, management considers the risk of override of controls, and the board (or the audit committee) oversees this assessment.

## Outsourced Service Providers (OSP)

As entities increase their reliance on OSPs, greater attention and oversight of third-party risk management is required to manage the resulting risks. Under the 2013 COSO Framework management should consider how OSPs are monitored.

# History of key internal control related events

A recent confluence of regulatory and standard-setting activities has elevated ICFR as a key area of focus for institutions, audit committees, auditors and regulators.



# COSO Guidance and Framework Overview

# COSO guidance

## The 2013 COSO Framework includes:

- **Executive Summary**
- **Internal Control — Integrated Framework (2013 Framework)**
- **Illustrative Tools for Assessing Effectiveness of a System of Internal Control**
- **Internal Control over External Financial Reporting: A Compendium of Approaches and Examples**

## Other COSO documents:

- **Guidance on Monitoring Internal Control Systems**
- **Enterprise Risk Management — Integrated Framework**

# Transition and terminology

## COSO transition guidance:

- 1992 Framework considered superseded after December 15, 2014

### SEC

- The SEC has not issued formal transition guidance.
- SEC rules require that a “suitable, recognized control framework that is established by a body or group that has followed due-process procedures, including the broad distribution of the framework for public comment” be used for purposes of management’s evaluation of Internal Controls over Financial Reporting (ICFR)
- SEC Chief Accountant Paul Beswick stated :  
“The “SEC staff plans to monitor the transition for issuers using the 1992 framework to evaluate whether, and if, any staff or Commission actions become necessary or appropriate at some point in the future. However, at this time, I’ll simply refer users of the COSO framework to the statements COSO has made about their new framework and their thoughts about transition.”
- SEC staff has further commented:  
“...the longer issuers continue to use the 1992 framework, the more likely they are to receive questions from the staff about whether the issuer’s use of the 1992 framework satisfies the SEC’s requirement to use a suitable, recognized framework (particularly after December 31, 2014...)”

### PCAOB

- PCAOB Auditing Standard No. 5 requires the auditor to use the same internal control framework used by management

# 2013 COSO Framework – principles and enhancements



## Use of principles to describe components

Component	Principles
Control Environment	<ol style="list-style-type: none"> <li>1. Demonstrates commitment to integrity and ethical values</li> <li>2. Board demonstrates independence and exercises oversight</li> <li>3. Management establishes structure, authority, and responsibility</li> <li>4. Organization demonstrates commitment to competence</li> <li>5. Enforces accountability</li> </ol>
	<p><b>Enhancements Include</b></p> <ul style="list-style-type: none"> <li>• Setting expectations for standards of conduct (with employees and OSPs), evaluating adherence to such standards, and addressing deviations in a timely manner</li> <li>• Matters related to board independence, skills and expertise</li> <li>• Importance of accountability for internal control</li> <li>• Planning and preparing for succession for those roles important to the effectiveness of internal control</li> <li>• Aligning incentives and rewards with internal control responsibilities</li> </ul>

# 2013 COSO Framework – principles and enhancements



## Use of principles to describe components

Component	Principles
<b>Risk Assessment</b>	6. Specifies relevant objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
	<b>Enhancements Include</b>
	<ul style="list-style-type: none"> <li>• Explains that the risk assessment process includes risk identification, analysis, and response</li> <li>• Considers velocity and persistence of risk (in addition to impact and likelihood)</li> <li>• Includes fraud risk assessment as a principle</li> <li>• Incorporates considerations of outsourced service providers</li> <li>• Importance of evaluating changes in the external environment, business model, operations, technology, relationships with OSPs, leadership and how such changes impact internal control</li> </ul>

# 2013 COSO Framework – principles and enhancements



## Use of principles to describe components

Component	Principles
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
	<b>Enhancements Include</b>
	<ul style="list-style-type: none"> <li>• Emphasis on the linkage between risk assessment and control activities</li> <li>• The types of control activities applied (including considering preventative vs. detective controls)</li> <li>• Incorporates updated technology concepts, including those related to technology infrastructure, security, acquisition, development, maintenance, and use of OSPs</li> <li>• Establishing responsibility and accountability for executing policies and procedures</li> <li>• Reassessing policies and procedures on a periodic basis to determine their continued relevance and if revisions are needed</li> </ul>

# 2013 COSO Framework – principles and enhancements



## Use of principles to describe components

Component	Principles
Information and Communication	13. Uses relevant and quality information 14. Communicates internally 15. Communicates externally
	<b>Enhancements Include</b>
	<ul style="list-style-type: none"> <li>• Identifying information requirements, verifying sources of data, processing relevant data, maintaining quality through processing, and using OSPs</li> <li>• Considering reliability and protection of data</li> <li>• Reevaluating information needs</li> <li>• Considering how information supports the functioning of internal control</li> <li>• Providing separate channels of communication for anonymous or confidential communication when normal communication channels are inoperative or ineffective (e.g., through whistle-blower hotlines)</li> </ul>

# 2013 COSO Framework – principles and enhancements



## Use of principles to describe components

Component	Principles
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies
	<b>Enhancements Include</b> <ul style="list-style-type: none"> <li>• Considerations of the rate of change when developing monitoring activities</li> <li>• Using a baseline of understanding to establish plans for ongoing and separate evaluations</li> <li>• Considerations related to monitoring at different levels of an organization and monitoring of OSPs</li> <li>• Using technology in the context of monitoring</li> <li>• Communicating deficiencies</li> <li>• Monitoring corrective actions</li> </ul>

# Internal Control Areas of Focus and Marketplace Observations

# ICFR: Areas of focus

ICFR hot topics	Cited in material weakness disclosures	Areas/ contributing factors to material fraud	Related 2013 COSO Framework principles
<b>Control Environment</b>			
Ethics program	✓	✓	1, 2
Delegation of authority			3
Competence and training of accounting personnel	✓		4
Establishing accountability and expectations for ICFR through performance and compensation systems			5
<b>Risk Assessment</b>			
Appropriateness of and support for accounting policies and procedures	✓		6
Detailed risk assessment for each relevant account and disclosure, and linking the risk assessment to related control activities			7, 10, 11, 12
Fraud risk assessment, including management override, financial statement manipulation, misappropriation of assets, and corruption		✓	8, 10, 11, 12
Revising the risk assessment and controls for one-time or infrequent transactions or events, such as: <ul style="list-style-type: none"> <li>• Significant changes in process, technology, or people</li> <li>• Business combinations</li> </ul>	✓	✓	9, 10, 11, 12

# ICFR: Areas of focus, cont.

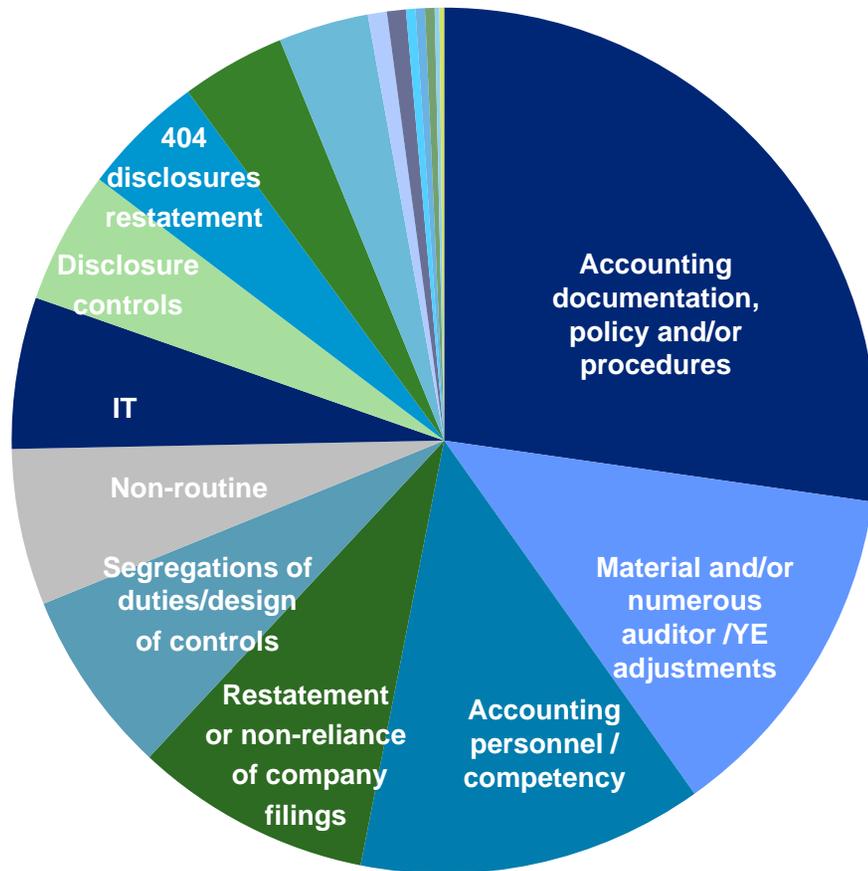
ICFR hot topics	Cited in material weakness disclosures	Areas/ contributing factors to material fraud	Related 2013 COSO Framework principles
<b>Control Activities</b>			
Establishing expectations through internal control policies and procedures			12
Journal entries	✓	✓	10
Segregation of duties such as IT system access issues and incompatible duties	✓	✓	10, 11
Account balance and disclosure specific controls, such as: <ul style="list-style-type: none"> <li>• Revenue</li> <li>• Inventory (including cycle count and/or physical inventory programs)</li> <li>• Taxes</li> <li>• Footnotes and cash flow statement</li> <li>• Account reconciliations</li> </ul>	✓	✓	10,12
Precision and evidence of management review controls, such as: <ul style="list-style-type: none"> <li>• Reserves, including inventory obsolescence, and bad debts</li> <li>• Impairment, including projections</li> <li>• Fair value of investments</li> <li>• Pension liabilities</li> <li>• Application of GAAP</li> <li>• Involving and/or overseeing specialists</li> <li>• Component financial results/data</li> </ul>	✓	✓	10, 12, 16
Use of outsourced service providers	✓		10, 12, 16
IT security and program change controls	✓		11

# ICFR: Areas of focus, cont.

ICFR hot topics	Cited in material weakness disclosures	Areas/ contributing factors to material fraud	Related 2013 COSO Framework principles
<b>Information and Communication</b>			
Quality of data, including reports used by controls			13
Whistleblower programs			14, 15
<b>Monitoring Activities</b>			
Monitoring approach linked to the risk assessment, including consideration of business units/locations		✓	16
Effectiveness and competence of the monitoring function, such as the internal audit function	✓	✓	16
Substance of the entity's periodic certification program			14, 15, 16
Evaluation of deficiencies to determine the root cause			17

# Data on Material Weaknesses

## Nature of Material Weakness Internal Control Issue

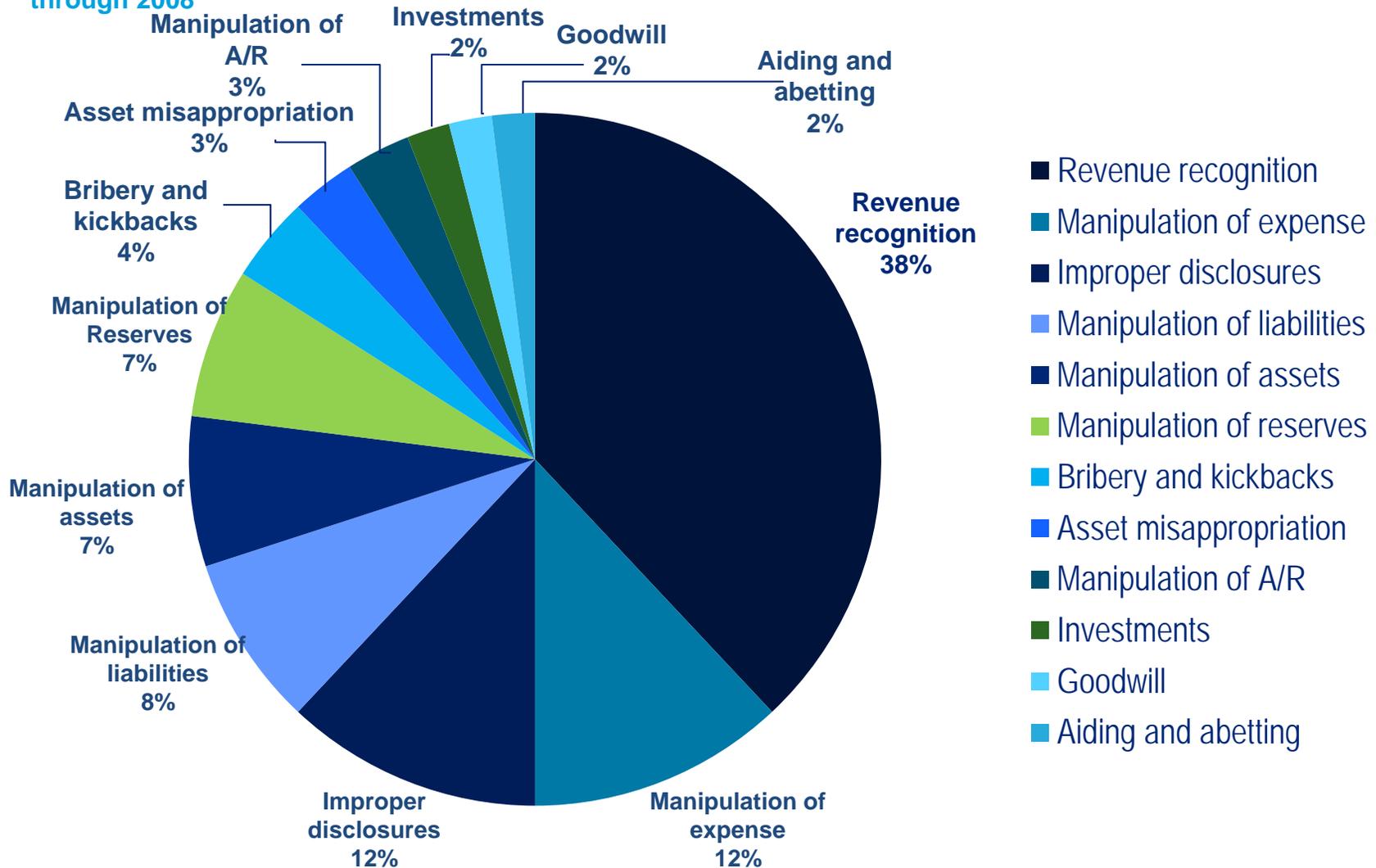


- Accounting documentation, policy and/or procedures
- Material and/or numerous auditor /YE adjustments
- Accounting personnel resources, competency/training
- Restatement or nonreliance of company filings
- Segregations of duties/ design of controls (personnel)
- Non-routine transaction control issues
- Information technology, software, security & access issue
- Inadequate disclosure controls
- Restatement of previous 404 disclosures
- Untimely or inadequate account reconciliations
- Journal entry control issues
- Ethical or compliance issues with personnel
- Treasury Control Issues
- Senior management competency, tone, reliability issues

Based on data from Audit Analytics for the period from November 15, 2012, through November 14, 2013, including 10-K filings for the calendar year ended December 31, 2012.

# Data on Material Fraud Issues

Proportion of financial statement fraud schemes represented by each alleged fraud scheme in AAERs from 2000 through 2008



Source: Deloitte Forensic Center, Ten Things About Financial Statement Fraud — third edition, 2009

# Marketplace observations

## What are we seeing and hearing...

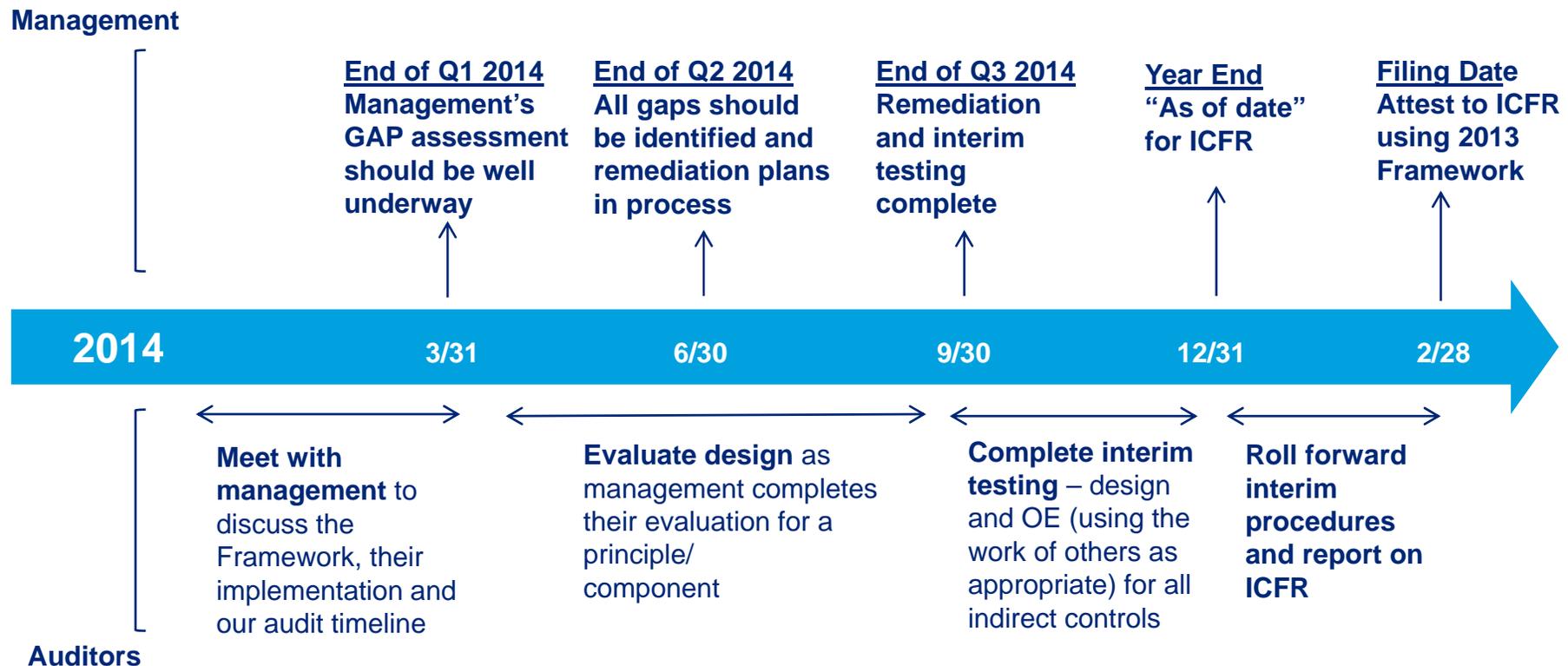
### Management:

- Discussing the Framework and implementation plans with their Board of Directors, audit committee, and internal and external auditors
  - Planning for adoption in 2014
  - Recognizing that this is more than just a mapping/documentation exercise
- Identifying GAPS or areas for improvement, particularly in the areas of significant change and hot topics
- Re-evaluating the documentation of their ICFR and the evidence of operation
- Considering how to leverage for operations and compliance

# Considerations and Next Steps

# Timeline for ICFR implementation (Assuming calendar year end company)

Companies need to focus on performing the gap assessment now, if they have not already started.



# Considerations and next steps

## Understand and educate

- Read 2013 Framework
- Identify new concepts and changes
- Consider training and education needs
- Discuss COSO update with the Board of Directors & Audit Committee

## Assess

- Assess and evaluate needs regarding control objectives for operations, compliance, and nonfinancial reporting
- Determine impacts on the entity's design and evaluation of ICFR
  - Assess coverage of the principles and consider points of focus
  - Assess current processes, activities, and available documentation regarding meeting the principles
  - Identify any control gaps or control testing enhancements
  - Reconsider testing, monitoring, and documentation

## Plan and implement

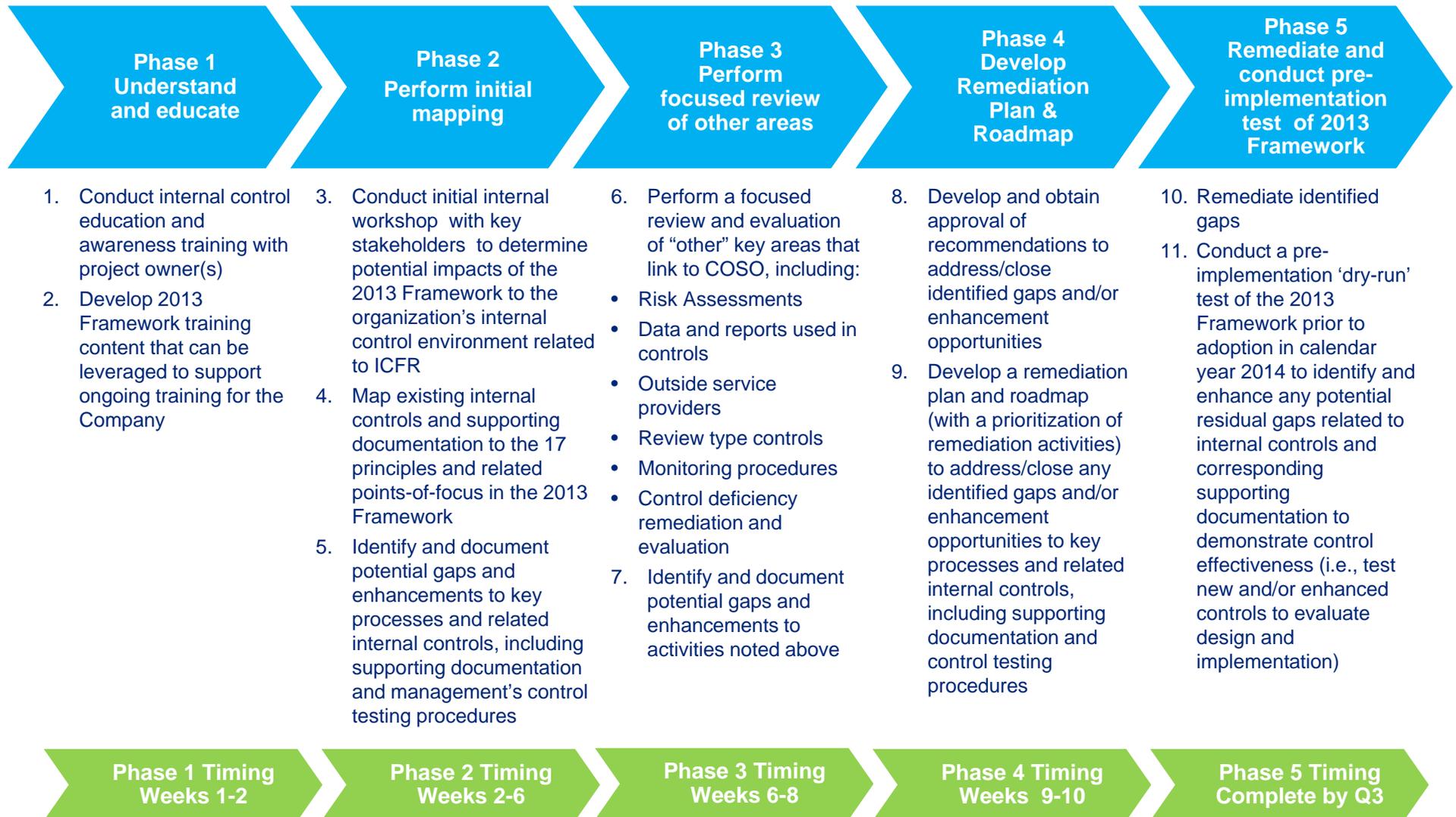
- Identify the steps that need to be performed to transition to the 2013 Framework
- Formulate a plan to transition
- Take appropriate steps to implement plan

## Communicate

- Communicate internally with all groups responsible for implementing, monitoring, and reporting on the organization's internal control
- Discuss and coordinate activities with internal audit (if applicable) and the external auditor

# Approach to Readiness Assessment

## Readiness Assessment Activities and Timing



# Resources

# How auditors can help

Area	Deloitte Offering
<b>Education and Training</b>	<ul style="list-style-type: none"> <li>• Educate Audit Committee and C-Suite on new COSO Framework               <ul style="list-style-type: none"> <li>• Dbriefs and Heads Up documents</li> <li>• Controller and Chief Audit Executive roundtables</li> <li>• One, four and eight hour new COSO learning programs</li> </ul> </li> </ul>
<b>Readiness/Gap Assessment</b>	<ul style="list-style-type: none"> <li>• Analyze current state processes, control activities and available internal control documentation with new COSO Framework elements</li> <li>• Provide advice and recommendations on potential gaps, including potential efficiencies and enhancements to business and IT processes.</li> </ul>
<b>Implement Controls or Process Improvements*</b>	<ul style="list-style-type: none"> <li>• Provide advice and recommendations as management implements new processes and controls or enhances existing processes and controls in areas such as:               <ul style="list-style-type: none"> <li>• Risk assessment, including fraud risk assessment</li> <li>• Information quality, including Information Produced by the Entity (IPE)</li> <li>• Monitoring and oversight of third party service providers</li> <li>• Precision of management review type controls</li> <li>• Use of analytics in the context of control activities and monitoring.</li> </ul> </li> </ul>
<b>Integrate New COSO into Other Functions</b>	<ul style="list-style-type: none"> <li>• Analyze the effectiveness of other functions (e.g., Internal Audit, Regulatory) in meeting the requirements outlined in new COSO Framework</li> <li>• Provide advice and recommendations to the function in integrating the new COSO Framework into existing processes, methods and documentation</li> <li>• Advise management on potential opportunities to leverage new COSO Framework in other operational or compliance functions</li> </ul>

\* If an Attest client, principally in operations or other compliance areas, not financial reporting.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

# Key resources

## Deloitte. Heads Up

June 10, 2013  
Volume 20, Issue 17

### In This Issue:

- Enhancements in the 2013 Framework
- Effective Systems of Internal Control
- COSO Transition Guidance and Impact on Other COSO Documents
- Internal Control Over External Financial Reporting
- Illustrative Tools
- Appendix A — Comparison of Principles in the 2013 Framework With Related Sections in the 1992 Framework, and Summary of Enhanced Concepts in the 2013 Framework
- Appendix B — Summary of Concepts and Discussion in the 2013 Framework Related to the Use of Outsourced Service Providers
- Appendix C — Summary of Concepts and Discussion in the 2013 Framework Related to Information Technology

### COSO Enhances Its *Internal Control — Integrated Framework*

by Jennifer Burns and Brent Simer, Deloitte LLP

On May 14, 2013, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) released an updated version of its *Internal Control — Integrated Framework* (the "2013 Framework"). In addition, COSO released two illustrative documents, *Illustrative Tools for Assessing Effectiveness of a System of Internal Control* (the "Illustrative Tools") and *Internal Control Over External Financial Reporting: A Compendium of Approaches and Examples* (the "ICEFR Compendium") as well as an executive summary of the 2013 Framework.

Originally issued in 1992, COSO's *Internal Control — Integrated Framework* (the "1992 Framework") became one of the most widely accepted internal control frameworks in the world. COSO's primary objective in updating and enhancing the framework is to address the significant changes to business and operating environments that have taken place over the past 20 years.

The 2013 Framework and Illustrative Tools can be purchased from the AICPA Store. An executive summary of the 2013 Framework is available for free on COSO's Web site.

This *Heads Up* provides an overview of the enhancements in the 2013 Framework, a discussion of considerations for entities that use the 1992 Framework in complying with Section 404 of the Sarbanes-Oxley Act of 2002 (SOX), and information about making the transition from the 1992 Framework to the 2013 Framework, including impacts on other COSO-related documents. In addition, the appendices to this *Heads Up* compare the 2013 Framework with the 1992 Framework as well as highlight some of the expanded concepts in the 2013 Framework. For additional information about the frameworks, see Deloitte's February 6, 2012, and August 7, 2012, *Heads Up* newsletters.

#### Enhancements in the 2013 Framework

The 2013 Framework creates a more formal structure for designing and evaluating the effectiveness of internal control by:

1. *Using principles to describe the components of internal control* — The 2013 Framework contains 17 principles that explain the concepts associated with the five components of the COSO Framework (control environment, risk assessment, control activities, information and communication, and monitoring activities). In developing the 17 principles, COSO focused on concepts from the 1992 Framework; considered the principles that were developed and articulated in COSO's 2006 *Internal Control Over Financial Reporting — Guidance for Smaller*

<sup>1</sup> COSO is a joint initiative of five private-sector organizations and is dedicated to providing thought leadership by developing frameworks and guidance on enterprise risk management, internal control, and fraud deterrence. The five private-sector organizations are the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, the Institute of Management Accountants, and the Institute of Internal Auditors.

## Resources

### • Deloitte Heads Up

- [www.Deloitte.com](http://www.Deloitte.com)

### • Deloitte Audit Committee Brief, March 2014

- [www.Deloitte.com](http://www.Deloitte.com)

### • The Framework and Tools are available for purchase through link on COSO website:

- [www.coso.org](http://www.coso.org)

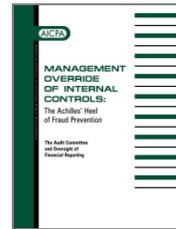
# Additional resources



## Audit Committee Brief

This issue of the Audit Committee Brief highlights hot topics related to internal control over financial reporting in light of the issuance of the Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) updated 2013 Internal Control — Integrated Framework (2013 COSO Framework).

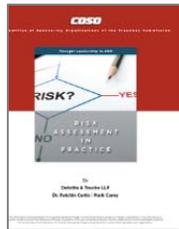
Published: March 2014 | Copies are available [here](#)



## AICPA: Management Override of Internal Controls: The Achilles' heel of Fraud Prevention

Published by the American Institute of Certified Public Accountants to offer guidance to audit committees in addressing the risk of fraud through management override of internal control over financial reporting

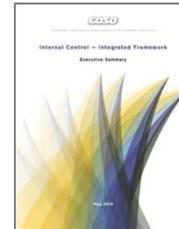
Published: 2005 | Copies are available [here](#)



## COSO Risk Assessment in Practice

This whitepaper developed by COSO, with contributions by Deloitte, presents a process for developing a risk assessment criteria, assessing risks and risk interactions, as well as prioritizing risks. It also discusses how to actually put this process into practice in a simple, practical and easy to understand way.

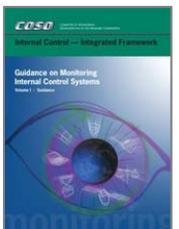
Published: October 2012 | Copies are available [here](#)



## COSO Enterprise Risk Management – Integrated Framework

This whitepaper, developed by COSO, focuses on the broader subject of enterprise risk management, while incorporating the internal control framework.

Published: 2004 | Copies are available [here](#)



## COSO Monitoring Guidance

This whitepaper, developed by COSO, explains monitoring guidance on internal controls, which is not superseded or affected by the 2013 Framework.

Published: 2009 | Copies are available [here](#)



## Deterrence and Detecting Financial Reporting Fraud

This report was published by the Center for Audit Quality (CAQ) and focuses on financial reporting fraud at publicly-traded companies of all sizes, and its recommendations are intended to be scalable to different situations.

Published: October 2010 | Copies are available [here](#)

# Additional resources, cont.



## Blind Spot

This paper outlines how finances can lead the way in the customer-centric bank.

Published: November 2012 | Copies are available in [PDF](#)



## Exploring Strategic Risk

The findings in this report are based on a global survey conducted in the spring of 2013 by Forbes Insights, on behalf of Deloitte. Business executives around the world say their understanding of the universe of strategic risk is changing.

Published: 2013 | Copies are available [here](#).



## Framing the future of corporate governance: Deloitte Governance Framework

The Center for Corporate Governance orchestrates dialogue, knowledge sharing, and thought leadership on governance issues to help advance collaboration among corporations, board members, the accounting profession, academia, and government.

Published: February 2013 | Copies are available in [PDF](#)



## Aftershock: Adjusting to the new world of risk management

Read the survey report by Deloitte and Forbes Insights which details the responses of 192 executives on how they are responding to a volatile, highly changeable risk environment.

Published: June 2012 | Copies are available in [PDF](#)



## Supply Chain Resilience: A Risk Intelligent approach to managing global supply chains

This publication is the 25th whitepaper in Deloitte's series on Risk Intelligence. The concepts and viewpoints presented build upon those in the first whitepaper in the series, The Risk Intelligent Enterprise™: ERM Done Right, as well as subsequent titles.

Published: May 2012 | Copies are available in [PDF](#)



This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

Copyright © 2014 Deloitte Development LLC. All rights reserved.  
36 USC 220506  
Member of Deloitte Touche Tohmatsu Limited