# COSO 2013: Moving from Five Principles to Seventeen

Steve Shofner, Senior Manager, Armanino

Core Competencies – C13

ISACA®
Trust in, and value from, information systems
San Francisco Chapter
2014 Fall Conference - "Think Big"
CRISC
CGEIT
CISM
CISA

# Learning Objectives

- Review the background of Internal Control Frameworks and why they are necessary in corporate environments.
- Review The Original COSO Framework
- Discuss how changes in the Governance, Risk, & Compliance (GRC) landscape have prompted changes to leading Frameworks
- Revised the revised COSO Framework and how changes impact your organization
- Implementation Roadmap: Identifying practical steps for the adoption of the new COSO Internal Controls framework.

# History of Controls Frameworks

# History of Controls Frameworks

- 1929: Wall Street Crash
- 1934: US Security and Exchange Commission (SEC) was formed
  - Public Companies are now *required* to perform annual audits

# History of Controls Frameworks

- 1987: The Committee Of Sponsoring Organizations (COSO) of the Treadway Commission, in response to corrupt mid-1970s accounting practices, funds a project to create an accounting control framework, including recommendations for Auditors, SEC, & Others

SPONSORING ORGANIZATIONS:

American Accounting Association | Thought Leaders in Accounting

AICPA American Institute of CPAs

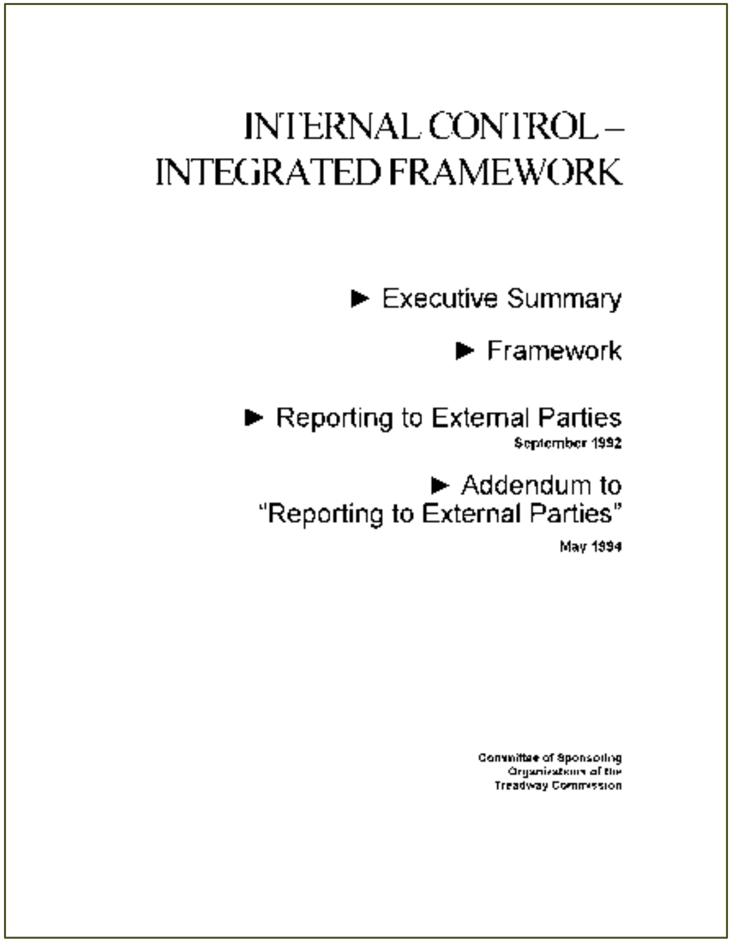
fei Financial Executives International

ima The Association of Accountants and Financial Professionals in Business

IIA The Institute of Internal Auditors

# History of Controls Frameworks

- 1992: “Internal Control – Integrated Framework,” a four-volume report, was released by the Committee of Sponsoring Organizations (COSO)
- *Per CFO Magazine, COSO used by 82% of survey respondents*



INTERNAL CONTROL – INTEGRATED FRAMEWORK

▶ Executive Summary

▶ Framework

▶ Reporting to External Parties
September 1992

▶ Addendum to “Reporting to External Parties”
May 1994

Committee of Sponsoring
Organizations of the
Treadway Commission

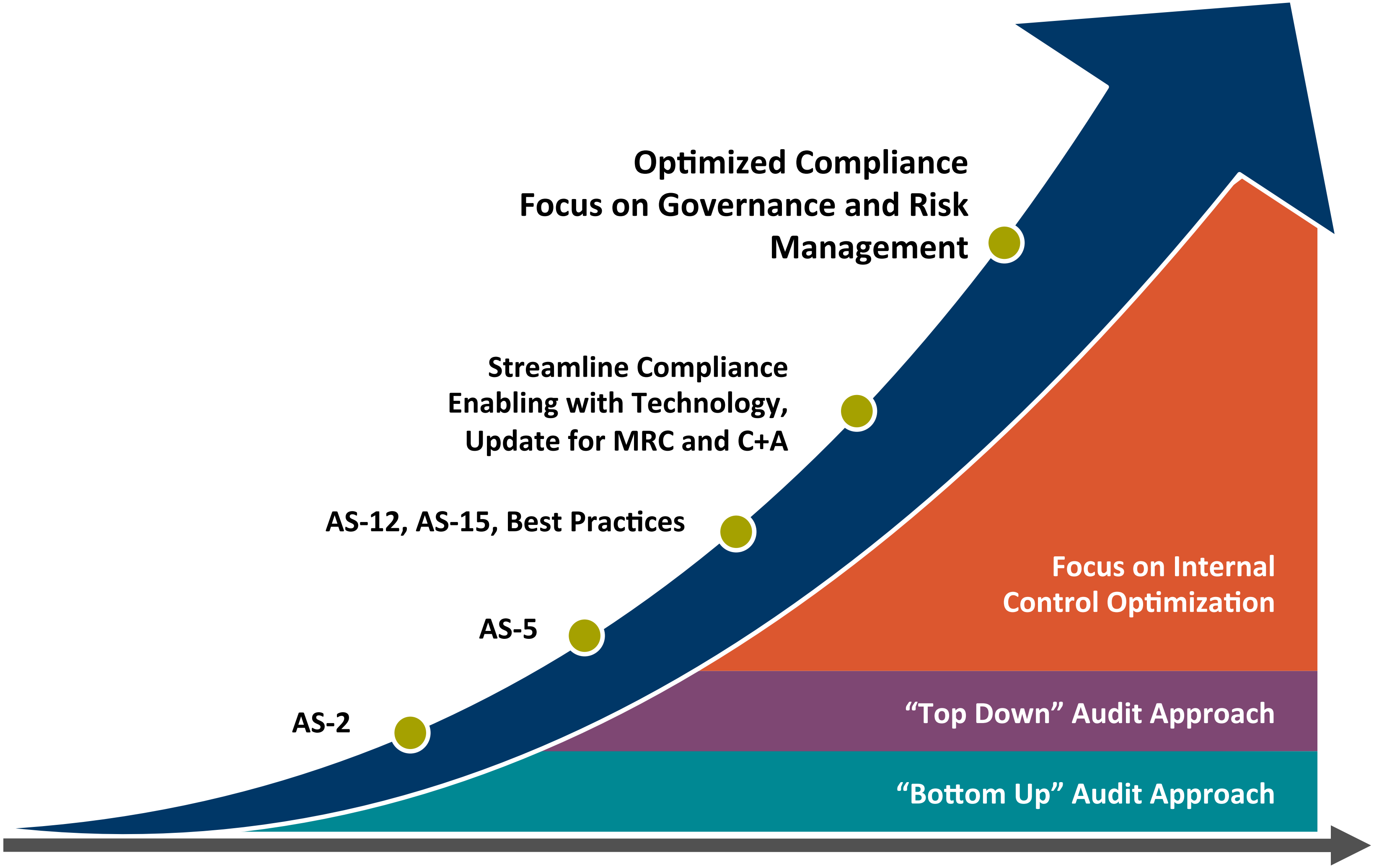
# History of Controls Frameworks

- *1996: Information Technology Governance Institute (ITGI) releases the Control Objectives for Information and Related Technology (COBIT) Framework*

# History of Controls Frameworks

- 2002: Sarbanes-Oxley (SOX) Act Passed, requiring companies to adopt and declare a framework used to define and assess internal controls
  - Section 404
    - Establish and maintain system of Internal Controls
    - Assess effectiveness annually
  - Created the Public Company Accounting Oversight Board (PCAOB), who codified standards:
    - PCAOB Auditing Standard 5 - Paragraph 5
      - Management and External Auditors to Use the Same Internal Control Framework
      - They specifically mention COSO as an option.

# The Evolving GRC Landscape



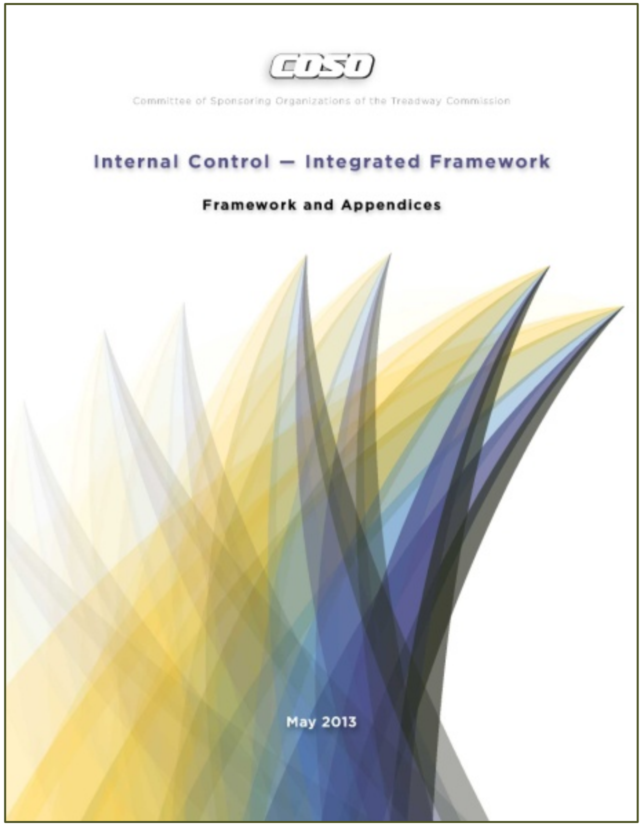
Optimized Compliance
Focus on Governance and Risk Management
Streamline Compliance
Enabling with Technology, Update for MRC and C+A
AS-12, AS-15, Best Practices
AS-5
AS-2
Focus on Internal Control Optimization
“Top Down” Audit Approach
“Bottom Up” Audit Approach

# Need For Updates

- Original COSO 20 Years Old
- Technology and Associated Risks Evolved
- Corporate Governance and Expectations Evolved
- Increased Focus on Risk Assessments
- Increased Organizational Interdependence
  - Joint Ventures
  - Supply Chain Dependencies
- Increased Importance of Compliance/ Operating Activities

# New COSO Internal Control Framework

- New COSO Internal Control-Integrated Framework
  - – Published May 2013
  - – Three Volumes + Separate Executive Summary (Combined 500 pages)
  - – Update to Original Framework
  - – Expands on five original components with 17 supporting (and required) principles



COSO

Committee of Sponsoring Organizations of the Treadway Commission

Internal Control — Integrated Framework

Framework and Appendices

May 2013

# COSO Overview

ISACA®
Trust in, and value from, information systems
San Francisco Chapter
CRISC
CGEIT
CISM
CISA
2014 Fall Conference - "Think Big"

# COSO Framework

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring

# “Environmental Controls” or “Entity-Level Controls” or “Governance”

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

# Control Environment

- Sets the tone of an organization, influencing the control consciousness of its people
- Is the foundation for all other components of internal control
- Provides discipline and structure
- Factors include:
  - The integrity, ethical values and competence of the entity's people;
  - Management's philosophy and operating style;
  - The way management assigns authority and responsibility, and organizes and develops its people;
  - The attention and direction provided by the board of directors.

# Risk Assessment

- Evaluates risks from external and internal sources, through the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed
- Economic, industry, regulatory and operating conditions will continue to change

# Information and Communication

- Pertinent information must be identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities.
- "Information systems" (not necessarily *technology*) produce reports containing operational, financial and compliance-related information that make it possible to run and control the business.
- Information needs to flow up, down, and across the organization

# Monitoring

- Monitoring of internal control effectiveness
- Accomplished through ongoing monitoring activities, separate evaluations or a combination of the two

# Control Activities (Financial)

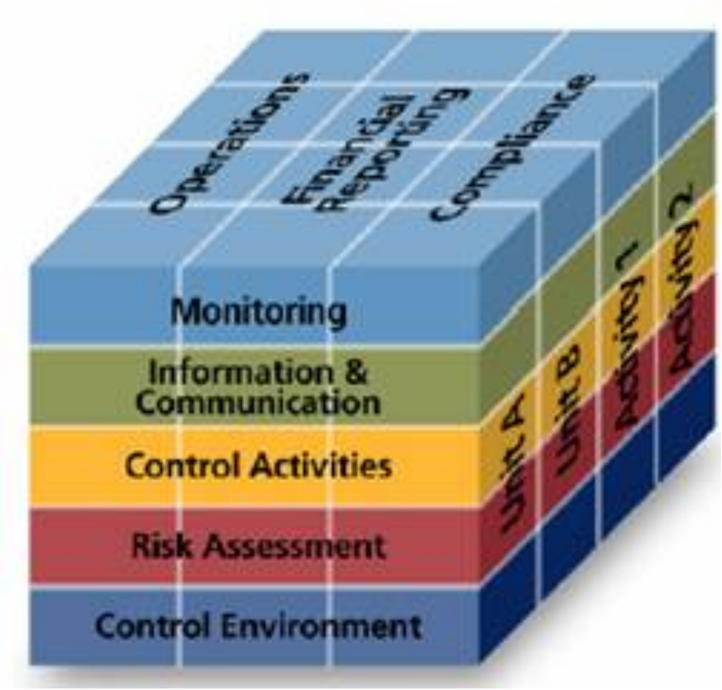
| Financial Statement Assertions (per PCAOB AS 15) | PCAOB Description (per PCAOB AS 15) | What does that mean? | Transactions are / were: |
|---|---|---|---|
| **Existence or Occurrence** | Assets or liabilities of the company exist at a given date, and recorded transactions have occurred during a given period | • Were transactions fictitious (perhaps to hide fraud)?<br>• Were transactions recorded in the proper time period (especially at period ends)? | • Real<br>• Timely |
| **Completeness** | All transactions and accounts that should be presented in the financial statements are so included | • Were all transactions included in totals?<br>• Were any transactions left out or missed?<br>• Mergers & acquisitions<br>• Business units<br>• Weeks / months in a quarter<br>• Different transaction types<br>• Were any transactions duplicated? | • Complete |
| **Valuation or Allocation** | Asset, liability, equity, revenue, and expense components have been included in the financial statements at appropriate amounts | • Were transactions misclassified to the wrong accounts (asset vs. expense vs. liability)?<br>• Was amortization and depreciation calculated correctly?<br>• Were any other calculations performed accurately? | • Classified<br>• Accurate |
| **Rights and Obligations** | The company holds or controls rights to the assets, and liabilities are obligations of the company at a given date. | • When appropriate, were transactions approved (spending limits, purchased from authorized vendors, sold to approved customers, credit limits not exceeded, etc.)?<br>• Were transactions valid (not sold to deceased, not shipped to outer space, didn't sell assets the company doesn't own, etc.)? | • Valid<br>• Authorized |
| **Presentation and Disclosure** | The components of the financial statements are properly classified, described, and disclosed | • Were financial statements fully disclosed (the truth, the whole truth, and nothing but the truth)? | • Fully presented and disclosed |

# Control Activities (IT)

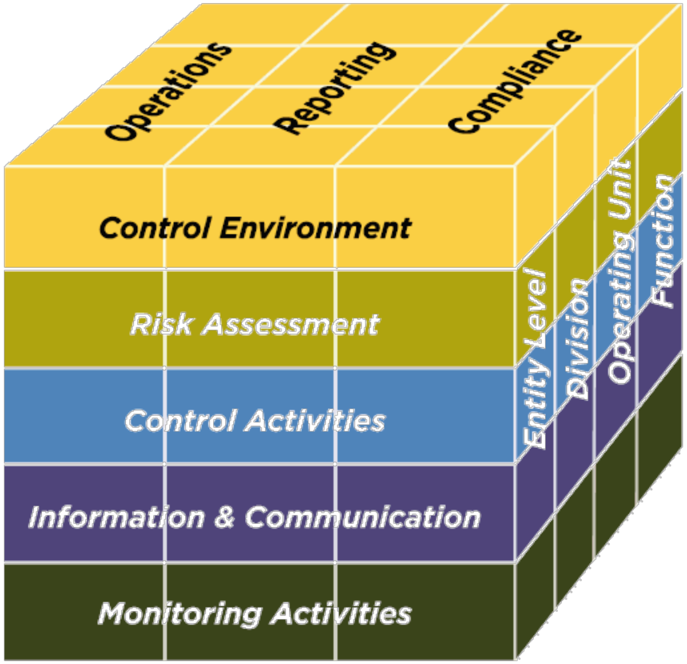
| IT Assertions | Description | Control Examples |
|---|---|---|
| **Secure** | IT systems are not accessible by non-authorized individuals, both inside and outside of the organization. This should include a combination of prevent, detect, and correct controls. | • Unique usernames<br>• Passwords<br>• Firewalls<br>• Intrusion Detection Systems |
| **Available** | IT systems are 'up' and running when needed. | • Monitoring<br>• Problem / Incident Response |
| **Confidential** | Data in IT systems is restricted to authorized individuals only. This is similar to Secure, above, but the focus is on data, not necessarily systems. | • Encryption |
| **Integrity** | IT systems perform their intended function correctly, completely, and timely. IT systems do not corrupt the data they process. | • Monitoring<br>• Problem / Incident Response |
| **Scalable** | IT systems can be expanded ('scaled') to meet the volume of processing needed. | • Automated 'spinning up' of new virtual machines to meet peak volume, such as holiday shopping.<br>• Capacity monitoring and response |
| **Reliable** | IT systems consistently perform their function complete, accurately, and timely. | • Change management (testing) |
| **Effective** | IT systems achieve their designed purpose. | • Any business-related control, such as a 3-way match between PO, receipt of goods, and invoicing. Then, the system kicks out a check. |
| **Efficient** | IT systems enable the organization to complete their tasks with greater quality, less expensively, or faster ('better, cheaper, faster). | • Any control focused on 'better, cheaper, faster." |

# The Revised COSO Framework

# Migration from 1992 to 2003 Framework



COSO Version 1992



COSO Version 2013

# COSO 2013's 17 Principles

| | |
|---|---|
| **Control Environment** | 1. Demonstrates commitment to integrity and ethical values<br>2. Exercises oversight responsibility<br>3. Establishes structure, authority and responsibility<br>4. Demonstrates commitment to competence<br>5. Enforces accountability |
| **Risk Assessment** | 6. Specifies suitable objectives<br>7. Identifies and analyzes risk<br>8. Assesses fraud risk<br>9. Identifies and analyzes significant change |
| **Control Activities** | 10. Selects and develops control activities<br>11. Selects and develops general controls over technology<br>12. Deploys through policies and procedures |
| **Information & Communication** | 13. Uses relevant information<br>14. Communicates internally<br>15. Communicates externally |
| **Monitoring Activities** | 16. Conducts ongoing and/or separate evaluations<br>17. Evaluates and communicates deficiencies |

**Note**: Each Principle is supported by Points of Focus

# COSO Points of Focus

- Aid Control Design by Describing How Principles are in Place
- Not Every Point of Focus Needs to Exist for Effective Internal Control

# Point of Focus Example

- Example of Point of Focus
- Component:
  - Control Environment
- Principle 1
  - The Organization demonstrates a commitment to integrity and ethical values
- Supporting Points of Focus
  - Sets the tone at the top
  - Establishes standards of conduct
  - Evaluates adherence to standards of conduct
  - Addresses deviations in a timely manner

# Key Changes

- Applies Principles-Based Approach
- More Formal Approach to Design & Evaluate Internal Controls
- Expands Reporting Category of Objectives
- Considers Different Business Models and Organizational Structures

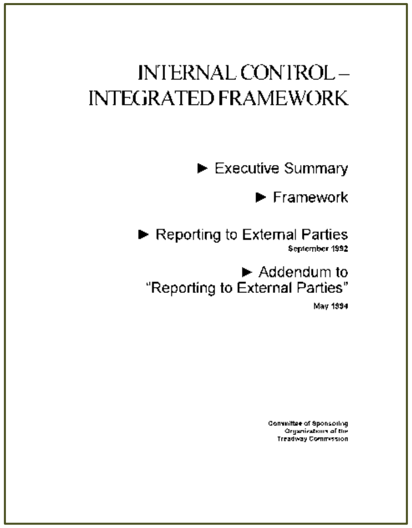
# Key Changes

- Clarifies Requirements for Effective Controls
- Reflects the Increased Relevance of Technology
- Enhances Governance Concepts

# Implementation Roadmap

# New Impact to Public Disclosures

- Additional Disclosure Requirement During New COSO Transition Period May 14, 2013 to December 15, 2014
- In SOX 404 Reports on Internal Control Over Financial Reporting where COSO Framework is Referenced, Must Disclosure
  - If Using Original 1992 Version
  - If Using New 2013 Version



INTERNAL CONTROL – INTEGRATED FRAMEWORK

► Executive Summary

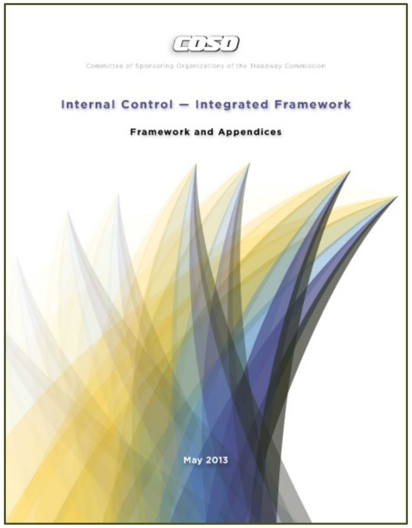
► Framework

► Reporting to External Parties
September 1992

► Addendum to "Reporting to External Parties"
May 1994

Committee of Sponsoring Organizations of the Treadway Commission

1992



COSO

Committee of Sponsoring Organizations of the Treadway Commission

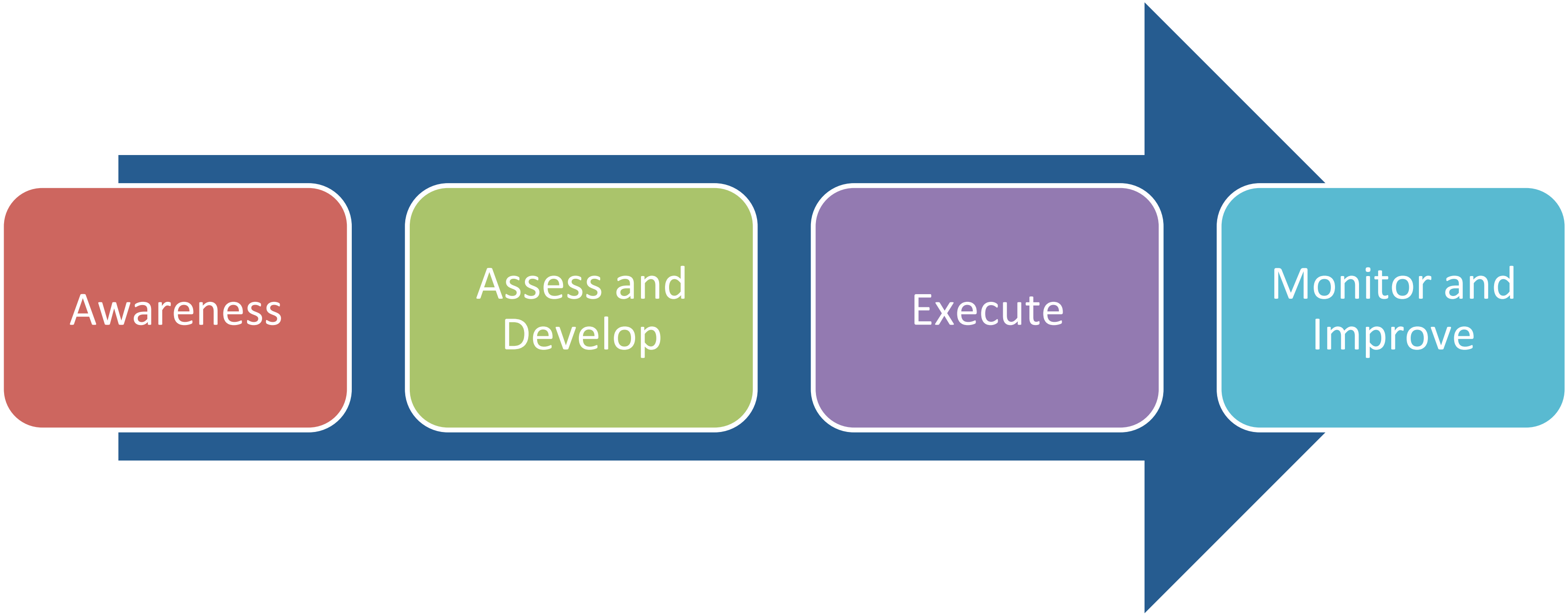
Internal Control — Integrated Framework

Framework and Appendices

May 2013

2013

# How to Comply



ISACA®
Trust in, and value from, information systems
San Francisco Chapter

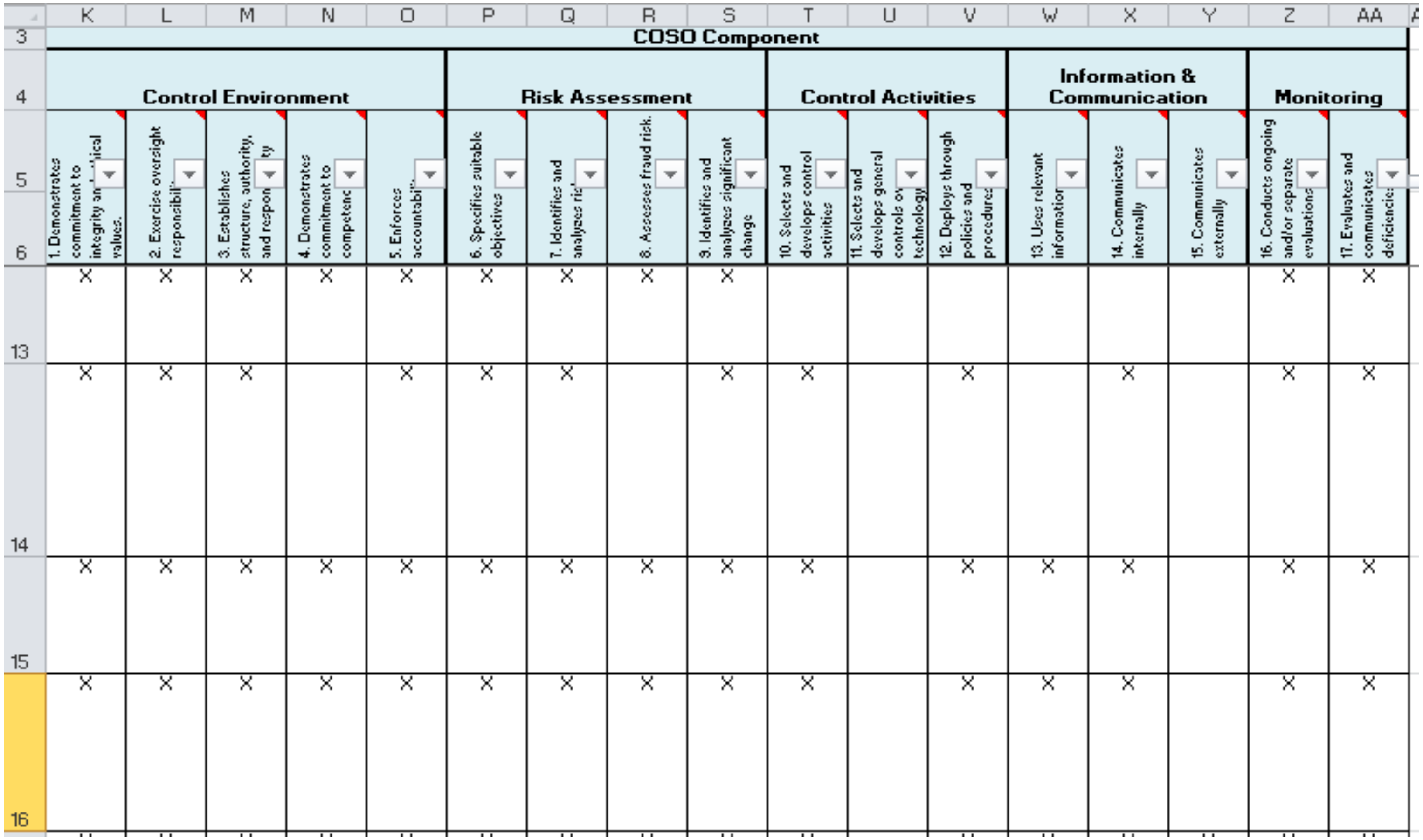
# Develop Awareness

- Adjust message for each audience
- Expanded Reporting Category
- Codified Principles
- Requirements of Effective Internal Control
- Internal Control Deficiencies
- Points of Focus

# Conduct Assessment

- Evaluate current environment and practices
- Evaluate the components of your internal "system"
  - People
  - Process
  - Technology
- Compare to COSO to identify gaps
- Leverage standard templates (where possible)
- Summarize results and develop Transition Plan

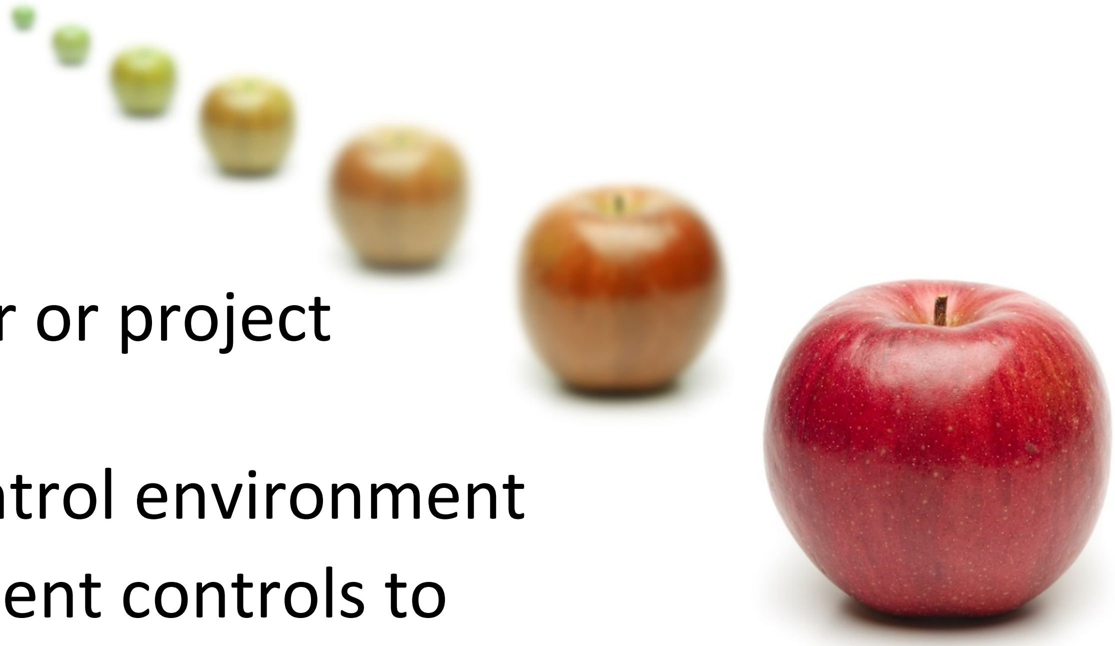
# Practical Considerations – Expand Risk Control Matrix



| | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | AA |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | COSO Component | | | | | | | | | | | | | | | | |
| 4 | Control Environment | | | | | Risk Assessment | | | | Control Activities | | | Information & Communication | | | Monitoring | |
| 5<br>6 | 1. Demonstrates commitment to integrity an ical values. | 2. Exercise oversight responsibil | 3. Establishes structure, authority, and respon ty | 4. Demonstrates commitment to competenc | 5. Enforces accountabi | 6. Specifies suitable objectives | 7. Identifies and analyzes ris | 8. Assesses fraud risk. | 9. Identifies and analyzes significant change | 10. Selects and develops control activities | 11. Selects and develops general controls ov technology | 12. Deploys through policies and procedure | 13. Uses relevant informatior | 14. Communicates internally | 15. Communicates externally | 16. Conducts ongoing and/or separate evaluations | 17. Evaluates and communicates deficiencie |
| 13 | X | X | X | X | X | X | X | X | X | | | | | | | X | X |
| 14 | X | X | X | | X | X | X | | X | X | | X | | X | | X | X |
| 15 | X | X | X | X | X | X | X | X | X | X | | X | X | X | | X | X |
| 16 | X | X | X | X | X | X | X | X | X | X | | X | X | X | | X | X |

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

# Execute Transition Plan



- Assign single owner or project manager
- Identify gaps in control environment
- Design and implement controls to address those gaps
- Design controls and processes to ensure your "system" is operating as intended

# Continuous Improvement

- Facilitate Broad Awareness
- Drive Continuous Improvement
- Evaluate Effectiveness
- Identify areas of inefficiency
- Review process and make updates

# How to Measure Compliance?

- All components of internal control framework are:
  - Designed appropriately to accomplish the control objective
  - Placed in operation
  - Operating effectively
- Provides reasonable assurance that the Organization:
  - Achieves effective and efficient operations when external events impacting objectives can be managed or mitigated to an acceptable level
  - Understands the extent operations are managed effectively and efficiently when external events impacting objectives cannot be mitigated to an acceptable level
  - Prepares reports following specific standards or objectives
  - Complies with applicable laws, rules and regulations

# Summary of Key Steps for Your Success With COSO 2013

- Map Existing Controls to 17 Principles
- Ensure Control Assessment Demonstrates
  - 17 Principles Are
    - Present
    - Functioning
  - 5 Components of Internal Control Are Integrated
    - Reduces Risk of Error or Misstatement to Acceptable Level
- Use 75 Points of Focus to
  - Ensure Control Design is Appropriate
  - Influence Tests of Control
- Disclose COSO Framework Utilized

# More Questions?

armanino

**Armanino**LLP **Certified Public Accountants & Consultants**

**Steve Shofner** office: 925.790.2879 mobile: 510.681.6638 email: steve.shofner@amllp.com