Updated COSO Framework & IIA Red Book Update

Internal Control - Integrated Framework 2013
Danny M. Goldberg

- Partner, Professional Development [www.sunera.com]
- Lead Professional Development and Executive Recruiting Practices Internationally for Sunera
- Founding Partner, SOFT GRC [www.thesoftaudit.com]
  - Sold to Sunera January 2011
- Former Director of Corporate Audit/SOX at Dr Pepper Snapple Group
- Former CAE - Tyler Technologies
- Published Author (Book/A rticles)
- Texas A&M University – 97/98
- CPA – Since 2000
- CIA – Since 2008
- CISA – Since 2008
- CGEIT (Certification in the Governance of Enterprise IT) – Since 2009
- CRISC (Certification in Risk and Information Systems Control) – Since 2011
- CRMA (Certification in Risk Management Assurance) – Since 2011
- CCSA (Certification in Control Self-Assessment) – Since 2007
- CGMA (Chartered Global Management Accountant) – Since 2012

Danny M. Goldberg (cont.)

- Chairman of the Leadership Council of the American Lung Association - North Texas – Calendar Year 2012
- Served on the Audit Committee of the Dallas Independent School District [CY 2008]
- Current Dallas and Fort Worth IIA Programs Co-Chair
- Published Author
  - Bureau of National Affairs - Internal Audit: Fundamental Principles and Best Practices [Professional Commentator]
  - ISACA Journal [May 2012, August 2012]
  - Internal Auditor Articles [August 2007, December 2007, October 2010]
  - ISACA Online Article [December 2009]
  - New Perspectives [December 2010]
Sunera Snapshot

Professional consultancy with core competency in:
- Internal Audit – IT Audit – Regulatory Compliance – PCI
- Finance & Accounting – Interim CFO/Controller – Training

Employ 175+ full-time professionals in 16 offices across the United States and Canada.

Founded in 2005, Sunera LLC has grown into the nation's largest independent provider of technology risk consulting.

PCI Qualified Security Assessor and Approved Scanning Vendor (QSA & ASV).

SAP Certified SAP integration partner with specific expertise in SAP security, GRC and controls.

ACL The only authorized reseller of ACL products in North America, solidifying our reputation as a market leader in Continuous Controls Monitoring.

Delivered more than 2,700 projects for 700 clients across all major industries and sectors. Sunera is adept in serving the Fortune 1000 but very adaptable to smaller organizations and government entities.

We deploy trained and certified professionals with appropriate oversight utilizing proven, pragmatic methodologies to ensure our teams deliver quality results.

We are solution oriented. Each project is tailored to your specific needs and our client-centric approach enables us to deploy teams that complement our clients’ internal capabilities.

We are known for completing projects that achieve anticipated benefits, on-time and within budget. Our rigorous project management discipline combined with our finance and IT capabilities enables us to successfully deliver a wide-range of projects.

Registered with NASBA to offer CPAs for our external Internal Audit and ACL training courses.

Sunera Offices

United States
- Atlanta
- Boston
- Chicago
- Dallas
- Denver
- Houston
- Los Angeles
- Miami
- New York
- Phoenix
- Raleigh
- San Francisco
- Tampa (Head Office)

Canada
- Calgary
- Toronto
- Vancouver
You can also visit us at www.sunera.com

Contact Information

Please contact any of the following Sunera Texas Leadership Team members:

Brian Amend
Managing Partner
Texas Practice
(972) 955-5652

Danny M. Goldberg
Partner, Professional Development
(214) 514-8883

Dallas Office Address
1400 Preston Road
Suite 400
Plano, Texas 75093

Houston Office Address
5100 Westheimer Road
Suite 200
Houston, Texas 77056

© 2012 Sunera LLC. All rights reserved.

COURSE OVERVIEW
Agenda

- COSO Update – Overview
  - History/Background
  - Changes Overview
  - Five Control Objectives
  - 17 Control Principles
  - Case Study: Developing a Checklist for Your Organization
- IIA Red Book Update
- Fraud Risk Assessment –
  - Overview
  - Key Steps
  - Interviewing and Brainstorming

Executive Update: Overview

- COSO Overview – Internal Control Publications

  1992  
  2006  
  2009  
  2013
Overview of COSO

- Committee of Sponsoring Organizations of the Treadway Commission (COSO)
  - Its major objective is to identify the factors that cause fraudulent financial reporting and to make recommendations to reduce its incidence.
  - COSO is sponsored by 5 main professional accounting organizations in the US:
    - American Institute of Certified Public Accountants (AICPA),
    - American Accounting Association (AAA),
    - Financial Executives Institute (FEI),
    - The Institute of Internal Auditors (IIA)
    - The Institute of Management Accountants (IMA).
- COSO has established a common definition of internal controls, standards, and criteria against which companies and organizations can assess their control systems.

Source: www.coso.org

Integrated Framework 2013

- Consists of three volumes:
  - Executive Summary
  - Framework and Appendices
  - Illustrative Tools for Assessing Effectiveness of a System of Internal Control
- Sets out:
  - Definition of internal control
  - Categories of objectives
  - Components and principles of internal control
  - Requirements for effectiveness

Copyright © 2013 COSO/ Sunera LLC
Why Update What Works

The Framework has become the most widely adopted control framework worldwide.

Original Framework

Refresh Objectives

Enhancements

Updated Framework


Reflect changes in business & operating environments

Expand operations and reporting objectives

Articulate principles to facilitate effective internal control

Updates Context

Broadens Application

Clarifies Requirements


Update expected to increase ease of use and broaden application

What is not changing...

• Core definition of internal control
• Three categories of objectives and five components of internal control
• Each of the five components of internal control are required for effective internal control
• Important role of judgment in designing, implementing and conducting internal control, and in assessing its effectiveness

What is changing...

• Changes in business and operating environments considered
• Operations and reporting objectives expanded
• Fundamental concepts underlying five components articulated as principles
• Additional approaches and examples relevant to operations, compliance, and non-financial reporting objectives added
The COSO Definition of Internal Control

Internal control is a process, effected by an entity’s board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

COSO Update - Executive Summary Highlights

- Provides a high level overview intended for the board of directors, chief executive officer, and other senior management.
- Applicable to all entities but the way in which it is implemented will be different for each organization (i.e., larger entities tend to be more formal and structured)
- Meant to assist stakeholders both internally and externally without being too prescriptive.
  - Accomplished by defining what constitutes a system of internal control and providing insight to when it is being applied effectively.
- Judgment is still a major factor in determining what is an effective system of internal control
  - To determine how much control is enough
  - To select, develop, and deploy controls across the entity
  - Management and internal auditors apply judgment as they monitor and assess the effectiveness of the system of internal control.
Executive Summary Highlights (continued)

- Requirements for an effective system of internal control are:
  - Each of the five components and relevant principles (17 principles in total) are present and functioning
  - The five components operate together in an integrated manner or as an integrated system
- When a major deficiency exists with respect to the presence and functioning of a component or relevant principle, or with respect to the components operating together in an integrated manner, the organization **cannot conclude** that it has met the requirements for an effective system of internal control.
- An effective system reduces, to an acceptable level, the risk of not achieving an entity objective and may relate to one, two, or all three categories of objectives (Operations, Reporting, Compliance)

Executive Summary Highlights (continued)

- Limitations do exist:
  - Suitability of objectives are a precondition to internal control
  - Human judgment can be faulty and subject to bias
  - Human failures such as simple errors do occur
  - Management could override internal control
  - Collusion could circumvent controls
  - External events beyond the organization’s control
- Internal control provides reasonable assurance of achieving the entity’s objectives but not absolute assurance
- Management should be aware of these limitations when selecting, developing, and deploying controls
Update Considers Changes in Business and Operating Environments

Environments changes...
- Expectations for governance oversight
- Globalization of markets and operations
- Changes and greater complexity in business
- Complexities in laws, rules, regulations, and standards
- Expectations for competencies and accountabilities
- Use of, and reliance on, evolving technologies
- Expectations relating to preventing and detecting fraud

...have driven Framework updates
- COSO Cube (2013 Edition)

Update Articulates 17 Principles of Effective Internal Control (to be discussed in more detail)

Control Environment (CE)
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 (RA)
6. Specifies suitable objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Identifies and analyzes significant change

Control Activities (CA)
10. Selects and develops control activities
11. Selects and develops general controls over technology
12. Deploys through policies and procedures

Information & Communication (IC)
13. Uses relevant information
14. Communicates internally
15. Communicates externally

Monitoring Activities (MA)
16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies
Update Clarifies Requirements for Effective Internal Control

- Effective internal control provides reasonable assurance regarding the achievement of objectives and requires that:
  - Each component and each relevant principle is present and functioning
  - The five components are operating together in an integrated manner
- Each principle is suitable to all entities; all principles are presumed relevant except in rare situations where management determines that a principle is not relevant to a component
- Components operate together when all components are present and functioning and internal control deficiencies aggregated across components do not result in one or more major deficiencies
- A major deficiency represents an internal control deficiency or combination thereof that severely reduces the likelihood that an entity can achieve its objectives

Update Describes Important Characteristics of Principles

- Points of focus may not be suitable or relevant, and others may be identified
- Points of focus may facilitate designing, implementing, and conducting internal control
- There is no requirement to separately assess whether points of focus are in place
Update Describes the Role of Controls to Effect Principles

- The Framework does not prescribe controls to be selected, developed, and deployed for effective internal control.
- An organization’s selection of controls to effect relevant principles and associated components is a function of management judgment based on factors unique to the entity.
- A major deficiency in a component or principle cannot be mitigated to an acceptable level by the presence and functioning of other components and principles.
- However, understanding and considering how controls effect multiple principles can provide persuasive evidence supporting management’s assessment of whether components and relevant principles are present and functioning.

ICEFR: A Compendium Overview

- Provides points of focus and approaches to satisfy each of the 17 principles of the Framework.
  - Points of Focus highlight key characteristics relating to each principle.
  - Approaches are summary-level descriptions of activities that management may consider as they apply the Framework in an ICEFR context.
- Examples are also provided to illustrate practical examples of how to apply principles, based on situations drawn from practical experience.
- Illustrates how various characteristics of principles may be present and functioning within a system of internal control relating to external financial reporting.
17 Principles of Effective Internal Control

Control Environment (CE)
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 (RA)
6. Specifies suitable objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Identifies and analyzes significant change

Control Activities (CA)
10. Selects and develops control activities
11. Selects and develops general controls over technology
12. Deploys through policies and procedures

Information & Communication (IC)
13. Uses relevant information
14. Communicates internally
15. Communicates externally

Monitoring Activities (MA)
16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies

GROUP EXERCISE
Group Exercise

- Break up groups based on industry
- For each of the Five Objectives, please read each of the Principles (17 in all) and create, as a group, a checklist of actions that a company would do in order to demonstrate each Principle and thus each Objective.
- 45 Minutes allotted to each of the 5 Objectives
Control Environment: Principles

1. The organization demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
Control Environment: Principle #1

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

1. Establishing Standards of Conduct

2. Leading by Example on Matters of Integrity and Ethics

3. Evaluating Management and Other Personnel, Outsourced Service Providers, and Business Partners for Adherence to Standards of Conduct

4. Developing Processes to Report and Promptly Act on Deviations from Standards of Conduct

---

P1: Approach - Establishing Standards of Conduct

- Communicating and reinforcing the accountability for responsible conduct of all personnel
- Permeating standards of conduct throughout the organization, including guidelines for application to high-risk issues and geographies
- Setting the expectation that personnel raise issues or questions relating to the application of the defined standards
- Making explicit the consequences for deviations from standards of conduct at any level in the organization
- Ensuring that new and existing employees are trained on the entity’s standards of conduct and continuing education, and providing appropriate briefings to third parties engaging in business with the company
- Developing performance evaluation processes and incentives (and service-level agreements as necessary) that promote the right behavior in pursuit of objectives
- Providing staff with ethics training opportunities to ensure that all employees have the knowledge to identify and deal with dilemmas

---

Copyright © 2013 COSO/ Sunera LLC
P1: Approach - Leading by Example on Matters of Integrity and Ethics

- Communications from senior management that support the expected standards of conduct and that stay consistent as the permeate the organization
- Day-to-day actions and decision making at all levels of the organization that are consistent with the expected standards of conduct
- Interactions with suppliers, customers, and other external parties that reflect fair and honest dealings (how is this determined?)
- Performance appraisals and incentives that reinforce expected standards of behavior consistent with the entity’s objectives at all levels of the organization
- Timely inquiries and investigations into any alleged conduct that is inconsistent with the entity’s standard of conduct

P1: Approach - Evaluating Mgmt & Other Personnel, Outsourced Service Providers, and Business Partners for Adherence to Standards of Conduct

- Considering anomalies in key performance indicators and internal analytical reviews of operational and financial information that could be a potential indicator of fraudulent financial reporting or other misconduct
- Considering the results from ongoing and separate evaluations of internal control, which includes evaluations of internal control at outsourced service providers and business partners who provide information necessary to produce external financial reporting
- Analyzing issues and trends from hotlines and help lines made available within the organization that indicate potential fraud occurrences and other ethical concerns
P1: Approach - Developing Processes to Report and Promptly Act on Deviations from Standards of Conduct

- Having individuals who are independent of the alleged matter conduct the investigation (depending on the significance, board-led investigation may be necessary)
- Applying criteria to prioritize deviations
- When applicable, assessing the financial statement impact and determining what internal controls over external financial reporting may have failed to detect the matter
- Identifying and communicating with anyone under investigation and following up on any corrective actions taken to remedy the matter in a consistent and timely basis and according to prescribed company guidelines
- Informing the board of deviations in the application of the standards and waivers that may have been granted or that are being considered
- Determining how and when the violation will be communicated and if it will be made public
- Communicating to all company personnel that appropriate investigation and corrective actions have been taken

Control Environment: Principle #2

The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
Principle #2: Approaches

1. Establishing the Roles, Responsibilities, and Delegation of Authority of the Board of Directors
2. Establishing P&P for Meetings between the BoD and Management
3. Identifying and Reviewing BoD Candidates
4. Reviewing Management’s Assertions and Judgments
5. Obtaining an External View
6. Considering Whistle-Blower Information about Financial Statement Errors and Irregularities

P2: Approach - Establishing the Roles, Responsibilities, and Delegation of Authority of the Board of Directors

The roles, responsibilities, and powers of delegation of the BoD are defined by its corporate bylaws and committee charters in accordance with applicable regulatory and listing requirements. For external financial reporting purposes, the board typically forms an audit committee, whose responsibilities include overseeing:

- Effectiveness of internal control over external financial reporting, including the assessment of risks, significant deficiencies, and material weaknesses (if any)
- Management’s assessment of any significant matters, considering the potential impact of financial reporting and need for corrective action
- The establishment of formal communication with management of the internal audit function to facilitate discussion of any sensitive issues
- The quality of financial reporting and disclosures
- The hiring and payment to the external auditor

Audit committee members typically demonstrate independence of thought and substance by absence of any material financial or other personal ties to the company, which could impede their ability to provide unbiased guidance and oversight.
P2: Approach - Establishing P&P for Meetings between the BoD and Management

The BoD reviews and approves P&P that support the performance of internal control across the business in regular meetings between management and the board. The processes and structure particularly relevant to the audit committee of the board are those that provide:

- Appropriate forums to enable board members to ask probing questions of management
- A calendar that establishes the timing and frequency of meeting with management
- Expected practices to keep board members current on both emerging and adopted accounting standards and their impact on the entity's financial statements (train and educate the Audit Committee!)
- Procedures to review management’s development and performance of internal control over external financial reporting
- Authority to engage experts as needed and oversight to ensure that management appropriately resolves matters raised by the board
- Criteria and procedures for calling special and/or urgent meetings as necessary
- Allocation of time in board meetings for discussions with external advisors, internal and external auditors, and legal counsel without management being present

P2: Approach - Identifying and Reviewing BoD Candidates

The BoD periodically assesses and confirms its collective ability to provide effective oversight. Through independent review and self-assessment it determines the adequacy of its composition, whether it has sufficient independent members, and the appropriate expertise.

To meet the entity’s external financial reporting objectives, the BoD identifies certain board candidates who are independent of both management and the entity and who have requisite financial reporting and other relevant expertise. These members are typically assisted to the audit committee. Such expertise may be established through professional networks and organizations and by educational institutions whose missions are aligned to the advancement of the financial reporting profession.
P2: Approach - Reviewing Management’s Assertions and Judgments

The Board demonstrates an appropriate level of skepticism of management’s assertions and judgments that affect financial reporting by asking probing questions. In particular, the audit committee of the board seeks clarification and justification of the company’s process for:

- Selecting and implementing accounting policies
- Determining critical accounting estimates
- Making key assumptions used in the application of technical accounting and reporting matters
- Evaluating other risks facing the organization, with the potential impact on financial reporting
- Confirm or reject the basis for management estimates and proposed accounting policy changes before approving
- Evaluate, retain, or change external auditors
- Review audit plans
- Review management’s assessment of internal control over external financial reporting

P2: Approach - Obtaining an External View

The audit committee of the board meets regularly with internal and external auditors as well as independent reviewers, in private when necessary, to review and discuss such topics as:

- Key risks facing the organization
- Audit scope and testing plans
- Basis for definition of materiality threshold
- Changes in accounting policies
- Assumptions in models and calculations
- Resources and staffing
- Organization and culture
- Management’s assessment of internal control over financial reporting
- Significant audit findings
- Quality and reliability of financial reporting and disclosures.
P2: Approach - Considering Whistle-Blower Information about Financial Statement Errors and Irregularities

The audit committee considers information obtained from the company’s whistle-blower and anti-fraud programs to monitor the risks in misstatements in financial reporting. These may include risks of inappropriate acts by staff and management override of controls. The audit committee reviews any whistle-blower allegations and evaluates management’s analysis of significant matters, potential impact on financial reporting, and corrective actions being taken.

Control Environment: Principle #3

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

1. Defining Rules and Reporting Lines and Assessing them for Relevance
2. Defining Authority at Different Levels of Management
3. Maintaining Job Descriptions and Service-Level Agreements
4. Defining the Role of Internal Auditors

P3: Approach - Defining Rules and Reporting Lines and Assessing them for Relevance

- Senior management prepares organizational charts to document, communicate, and enforce accountability for the achievement of the entity's financial reporting objectives. The org charts can be used to:
  - Set forth assignments of authority and responsibility
  - Ensure duties are appropriately segregated
  - Establish reporting lines and communication channels
  - Define the various reporting dimensions relevant to the organization
  - Identify dependencies for roles and responsibilities involved in financial reporting as well as those accountable for external parties
P3: Approach - Defining Authority at Different Levels of Management

- BoD outlines its oversight authority for financial reporting over senior management through its charter. When assigning authorities and responsibilities, management considers the impact on the control environment and the importance of effectively segregating duties. Policy documents define cascading levels of authority, checks, and balances for authorizing transactions, and accounting and reporting of financial results.
- Such authority and responsibility is deliberately limited in order to balance the need for the efficient achievement of objectives against the risks that could result from unmonitored inappropriate conduct. Management empowers employees to correct problems or implement improvements in their assigned business process as necessary.

P3: Approach - Maintaining Job Descriptions and Service-Level Agreements

- Based on the delegated authority levels, management maintains job descriptions to outline financial reporting responsibilities, and updates them when needed. In addition, management provides sufficient direction to ensure that employees recognize their responsibility for internal control and the importance of applying appropriate diligence and business judgment when they carry out their assigned job responsibilities.
- For key financial reporting positions, the BoD reviews management’s descriptions of the related authorities and responsibilities and considers how those positions affect the strength of internal control over external financial reporting.
- When applicable, the responsibilities of externally sourced support personnel are outlined through service-level agreements, specifically targeting timeliness and the quality of financial reports generated.
P3: Approach - Defining the Role of Internal Auditors

- In companies with formal internal audit functions, the board of directors empowers the IA function to carry out its purpose, authority, and responsibilities with direct access to the audit committee and/or the BoD. The board or audit committee is actively involved in reviewing the company’s risk assessment, ensuring that the IA plan provides adequate assurance on the adequacy of coverage of key risk areas, and overseeing the internal audit compensation to ensure it is structured in a manner that supports the need for objectivity.

Control Environment: Principle #4

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

1. Establishing Required Knowledge Skills, and Expertise
3. Identifying and Delivering Financial Reporting-Related Training as Needed
4. Selecting Appropriate Outsourced Service Providers
5. Evaluating Competence and Behavior
6. Evaluating the Capacity of Finance Personnel
7. Developing Alternate Candidate for Key Financial Reporting Roles

P4: Approach - Establishing Required Knowledge Skills, and Expertise

- The audit committee of the board reviews and approves the competency requirements of all individuals serving in key financial reporting and internal audit roles and for all members of the audit committee. These are based on applicable laws and regulations, and on the expertise needed for applying the entity’s existing P&P related to external financial reporting.
- Management develops and maintains P&P that reflect the organization’s values and objectives. For instance, job descriptions capture the expectations in terms of the knowledge, skills, expertise needed for to effectively carry out responsibilities for each f/r position.
- The finance department regularly reviews the entity’s accounting and reporting policies and practices, and updates these as necessary to keep pace with internal expectations and external factors, including changes in technical standards and regulatory requirements.
- The HR department periodically updates materials outlining the company’s policies and procedures on attracting, training, coaching, evaluating, and retaining personnel.

- P&P that represent the entity’s competence standards for financial reporting positions are used as a basis for HR and employee compliance activities, which may include:
  - Selecting and interviewing candidates
  - Performing background/reference checks
  - Making hiring, retention, promotion, and termination decisions
  - Developing training curricula
  - Setting certification expectations
  - Conducting exit interviews to uncover any concerns related to the entity’s internal control over external financial reporting.

P4: Approach - Identifying and Delivering Financial Reporting-Related Training as Needed

- Training needs are identified and delivered to targeted personnel. These address regulatory expectations, emerging accounting and reporting standards, and in-house input on areas that require improvement. Training needs are reprioritized as necessary in response to how often applicable changes occur, both within and outside the organization.
P4: Approach - Selecting Appropriate Outsourced Service Providers

- Management identifies the required skills and experience necessary to support the entity’s external financial reporting objectives. It then decides whether to internally retain people with the skills and experience or to outsource to a third party. Skills and experience matter with third parties but the entity’s policies on using vendors and on ethical standards.

P4: Approach - Evaluating Competence and Behavior

- To instill a common understanding and application of expected competence and behavioral standards, management consistently communicates expectations through policies and conducts practices and evaluates employee adherence by:
  - Developing incentives and rewards that consider the multiple dimensions of conduct and performance
  - Reinforcing expectations of continued demonstration and strengthening of expected levels of competence
  - Ensuring individual and team goals in support of the achievement of the entity’s objectives are defined, use observable measures, and are communicated to each employee.
  - Develop a performance appraisal process that confirms employee knowledge of both their progress against their goals and their status within the organization
  - Conducting periodic performance reviews and evaluating employees relative to their assigned roles to confirm that the employees’ skills are appropriate for their current job responsibilities
  - Making appropriate advancement or termination decisions based on performance reviews
P4: Approach - Evaluating the Capacity of Finance Personnel

- Senior Management evaluates the capacity of personnel who are involved in recording and reporting financial information, and in designing and developing financial reporting systems including underlying IT systems.
- Senior management assesses the department’s ability to identify issues, articulate positions supported by the relevant literature, and stay abreast of technical financial reporting developments. Considerations when assessing the adequacy of staffing levels and competence of financial reporting personnel include the extent of technical skills, nature and frequency of their training, workload, and the number of personnel dedicated to financial reporting.

P4: Approach - Developing Alternate Candidate for Key Financial Reporting Roles

- The BoD identifies the essential roles for the functioning of the business, including the CEO and CFO, deemed most important to the achievement of the entity’s financial reporting objectives.
- For each of those roles, management defines succession plans to ease any future transition and to mitigate the risk of not meeting financial reporting objectives. The BoD oversees this process to ensure that management has properly assessed and managed the risks associated with succession planning.
Control Environment: Principle #5

The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Principle #5: Approaches

1. Defining and Confirming Responsibilities
2. Developing Balanced Performance Measures, Incentives, and Rewards
3. Evaluating Performance Measures for Intended Influence
4. Approach Linking Compensation and Other Rewards
P5: Approach - Defining and Confirming Responsibilities

- Management develops descriptions of various roles to reinforce its responsibility for effective internal control over external financial reporting. In pursuit of the entity’s objectives, the BoD and senior management maintain a philosophy and operating style that demonstrate a strong commitment to ethics, integrity, and competence.
- Periodically, the CEO and CFO, as the parties ultimately responsible for internal control, request individuals within the entity to confirm accountability and represent that they have fulfilled their internal control responsibilities during any given period of time, highlighting any exceptions.

P5: Approach - Developing Balanced Performance Measures, Incentives, and Rewards

- Senior management defines performance measures, incentives, and rewards that are:
  - Aligned with the entity’s ethical values
  - Developed at all levels of the entity that management deems necessary to support and ensure accountability toward meeting both the entity’s short-term and longer-term objectives
  - Balanced to include both financial and non-financial measures
  - Incorporated into the entity’s hiring, evaluation, and promotion structures
- Senior management subsequently reports to the board what factors were considered in developing the performance measures, incentives, and rewards and how they are expected to drive the desired behavior.
P5: Approach - Evaluating Performance Measures for Intended Influence

- The BoD and management periodically evaluate the appropriateness of performance measures used to determine whether they have the intended influence on how people respond to pressures, incentives, and rewards. The evaluation may include:
  - Reassessing the relevance of performance measures considering industry trends, regulatory changes, or changes in the entity’s objectives
  - Considering past financial errors, ethical violations, and instances of non-compliance and whether the established measure could have caused excessive pressures to override controls.
  - Engaging external parties to conduct benchmarking and to interview employees
  - Monitoring the changing sources of threats that cause pressure to bypass established controls or take shortcuts
  - Considering whether the selection of accounting policies has been unduly influenced by the established performance measures
  - Using the assessment to make changes in performance measures and associated hiring, evaluation, and promotion structures

P5: Approach Linking Compensation and Other Rewards

- Management designs objective employee evaluation and compensation systems that periodically provide individual rewards, or disciplinary actions, as necessary. Decisions about both rewards and disciplinary actions are based on established objectives, including the individual’s adherence to the standards of conduct and performance toward the entity objectives regarding internal control over external financial reporting.
Risk Assessment

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.

9. The organization identifies and assesses changes that could significantly impact the system of internal control.
Risk Assessment: Principle #6

The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

Principle #6: Approaches

1. Identifying Financial Statement Accounts, Disclosure and Assertions
2. Specifying Financial Reporting Objectives
3. Assessing Materiality
4. Reviewing and Updating Understanding of Applicable Standards
5. Considering the Range of Activities

- Management specifies objectives relating to the preparation of financial statements, including disclosures, and identifies significant financial statement accounts based on the risk of material omission and misstatement.

- Management identifies, for each account and disclosure relevant assertions, underlying transactions and events, and processes supporting these financial statement accounts. The entity uses financial statement assertions relevant to its financial statement accounts and disclosures.

P6: Approach - Specifying Financial Reporting Objectives

- Management specifies a high-level financial reporting objective that forms the basis for all sub-objectives. In specifying objectives, management has documented objectives that are specific, measurable, attainable, relevant, and time-bound (SMART).

- Management, as part of internal control, assesses whether the objectives are consistent with accounting principles that are relevant for that entity and appropriate in the circumstances.
P6: Approach - Assessing Materiality

- Management assesses materiality of significant accounts, considering both quantitative and qualitative factors. In conducting this assessment, management may consider factors such as:
  - Who uses the financial statements
  - Size of financial statement elements
  - Uniqueness of the transactions
  - Difficulty in valuing the balance or specific transactions
  - Trends

[NOTE: Discuss with External Auditors]

P6: Approach - Reviewing and Updating Understanding of Applicable Standards

- Management reviews publications from professional bodies for updates in accounting pronouncements relevant to the business.
- Periodically, management presents to the audit committee an analysis of changes released or emerging issues that may significantly impact financial reporting and notes any significant differences from accounting policies of similar entities.

[NOTE: Discuss with External Auditors]
P6: Approach - Considering the Range of Activities

- Management, with oversight of the audit committee, considers the range of the entity’s activities to assess whether all material activities are appropriately captured in the financial statements.
- Management considers whether the presentation and disclosure of the financial statements enable the intended users to understand these material transactions and events.

Risk Assessment: Principle #7

The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
Principle #7: Approaches

1. Applying a Risk Identification Process
2. Assessing Risks to Significant Financial Statement Accounts
3. Assessing the Likelihood and Significance of Identified Risks
4. Considering Internal and External Factors
5. Evaluating Risk Responses

P7: Approach - Applying a Risk Identification Process

- Management includes a risk identification process that identifies risks of material omission and misstatement and the likelihood of occurrence of the risks to relevant financial statement assertions for each significant account and disclosure. In preparing this analysis, management considers the business processes and business units supporting financial statement accounts and disclosures.
- The process of identifying the supporting business units includes discussions with each business unit or process leader. It also includes identifying the information technology systems that support those business processes that are relevant to the external financial reporting objectives.
Management identifies risks to the achievement of financial reporting objectives by considering risk factors related to each significant financial statement account and the associated financial statement assertions. The process of identifying and analyzing risk considers both quantitative and qualitative factors, including the following:

- Impact on Financial Statement Accounts
- Account Characteristics
- Business Process Characteristics
- Fraud Risk
- Entity-Wide Factors

Management analyzes the significant of identified risks based on the likelihood of the risk occurring and the inherent risk of a material omission and misstatement to the entity’s external financial reporting objectives. Based on the outcomes of the analysis, management determines how to manage the risks to a tolerable level.
P7: Approach - Considering Internal and External Factors

- Management considers external factors that may impact the ability to achieve financial reporting objectives, such as:
  - Economic changes
  - Natural or human-caused catastrophes or environmental changes
  - New standards
  - Changes to laws and regulations
  - Changing customer demands
  - Technological developments

- Management considers internal factors that may impact the entity’s ability to achieve its financial reporting objectives, such as:
  - Use of capital resource determinations
  - Change in management responsibilities
  - Personnel hiring and training considerations
  - Employee accessibility to assets
  - Internal information technology changes

P7: Approach - Evaluating Risk Responses

- Management considers a variety of risk responses – avoid, accept, reduce, share – when evaluating whether risks are reduced to an acceptable level. In this process, management may consider unique risks related to financial reporting or a combination of risks.

- Management may also consider how risk responses impacting the five components of internal control interact to reduce risk to an acceptable level.
Risk Assessment: Principle #8

The organization considers the potential for fraud in assessing risks to the achievement of objectives.

Principle #8: Approaches

1. Conducting Fraud Risk Assessments
2. Considering Approaches to Circumvent or Override Controls
3. Reviewing Incentives and Pressures Related to Compensation Programs
P8: Approach - Conducting Fraud Risk Assessments

- Management conducts a comprehensive fraud risk assessment to identify the various ways that fraud and misconduct can occur, considering:
  - Degree of estimates and judgments in external financial reporting
  - Methodology for recording and calculating certain accounts (e.g., inventory)
  - Fraud schemes and scenarios that are common to the industry sectors and markets in which the entity operates
  - Geographic regions where the entity does business
  - Incentives that may motivate fraudulent behavior
  - Nature of automation
  - Unusual or complex transactions subject to significant management influence
  - Last-minute transactions
  - Vulnerability to management override and potential schemes to circumvent existing control activities
  (NOTE: Discussed in more detail later section)

P8: Approach - Considering Approaches to Circumvent or Override Controls

- Entity personnel, including management, may intentionally override controls in a number of ways, which may include:
  - Recording fictitious business events or transactions
  - Changing the timing of recognition of legitimate transactions (particularly those recorded close to the end of an accounting period)
  - Establishing or reversing reserves to manipulate results
  - Altering records and terms related to significant or unusual transactions
P8: Approach - Reviewing Incentives and Pressures Related to Compensation Programs

- Management considers how personnel may rationalize behavior regarding evaluations, compensation, or employment.
- Board and management review the entity's compensation programs and performance evaluation process to identify potential incentives and pressures for employees to commit fraud (should CAE's be on an incentive-compensation plan?)
- This review considers how meeting, or not meeting, financial reporting targets potentially impacts an individual's evaluation, compensation, and continued employment.

Risk Assessment: Principle #9

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

1. Assessing Change in the External Environment
2. Conducting Risk Assessments Relating to Significant Change
3. Considering Change Through Succession
4. Considering CEO and Senior Executive Changes

Management develops approaches for observing changes in the external market and assessing the potential impact on the entity’s operations and financial reporting. May include reviewing the following:

- Websites and social media
- Website tracking tools
- Newspaper clipping services
- Search engines
- Trade publications and trade shows
- Conferences
- Professional organizations
P9: Approach - Conducting Risk Assessments Relating to Significant Change

Following a decision to pursue a new business strategy or significantly change the current strategy, management conducts a detailed risk assessment to consider how the changes might impact the achievement of all objectives set across the entity.

P9: Approach - Considering Change Through Succession

As part of the overall succession process, management reviews planned changes in management and leadership positions and the attitudes and values portrayed by the incumbents to those positions through interviews with personnel within the entity.

[NOTE: How many organization have a formal succession plan?]
P9: Approach - Considering CEO and Senior Executive Changes

- The desired qualities relating to attitudes towards risk, risk tolerance, and internal controls are compiled as part of a comprehensive leadership profile to identify the “ideal” future CEO.
- Leadership profile is used to evaluate the potential candidates considered for the position.
- As part of recruiting for the CEO and other executive team members, the audit committee asks candidates to articulate its views on the importance of internal control and how it would balance the need for effective control with other pressures for performance and cost considerations.
- When assessing the internal candidates, the audit committee also considers the candidates’ track record on maintaining control and effectively managing the pressure to perform.
Control Activities

10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

11. The organization selects and develops general control activities over technology to support the achievement of objectives.

12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into place.
Control Activities: Principle #10

The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
Principle #10: Approaches

1. Using Matrices, Workshops, or an Inventory of Control Activities to Map Identified Risks to Control Activities
2. Implementing or Assessing Control Activities when Outsourcing to a Third Party
3. Considering the Types of Control Activities
4. Considering Alternative Control Activities to the Segregation of Duties
5. Identifying Incompatible Functions

P10: Approach - Using Matrices, Workshops, or an Inventory of Control Activities to Map Identified Risks to Control Activities

Once risks have been identified and mapped to relevant financial statements assertions, management determines relevant business processes and selects and develops control activities to address each risk [SOX testing?]. Includes those individuals responsible for the risk in their areas, finance personnel responsible for financial reporting, and other control experts, such as internal auditors or others who have relevant specialized knowledge. Centralized group responsible for financial reporting or control activities periodically reviews the risk control matrices to help ensure that the entity’s financial reporting risks are being addressed.
The organization outsources some of its operations to a third party, which may or may not issue a “report on controls at a service organization” following an appropriate local or international standard. Although the organization may rely on an outsourced service provider to conduct processes, policies, and procedures on behalf of the entity, management retains ultimate responsibility for designing, implementing, and conducting an effective and efficient system of internal control.

In determining the significance of the service organization’s processes to the financial statements, the entity considers the following factors (SSAE 16/SAS 70):

- The significance of the transactions or information processed by the service organization to the entity’s financial statements
- The risk of material omission and misstatement associated with the assertions affected by the processes of the service organization, including whether the activities involve assets that are susceptible to loss or misappropriation
- The nature and the complexity of the services provided by the service organization and whether they are highly standardized and used extensively by many organizations or unique and used only by a few

If management determines that the service organization’s processes are significant to internal control over external financial reporting, then it:

- Identifies the specific control activities performed by the service organization that are relevant to financial statement assertions, and/or
- Selects and develops control activities internally over the activities performed by the service organization

If a report on controls at a service organization is available, management can use it to determine what financially significant processes are covered, whether appropriate control activities are in place, and what control activities are required in its own organization to address external financial reporting risks.
P10: Approach - Considering the Types of Control Activities

Once risks have been identified and mapped to the relevant financial statement assertions, management determines relevant business processes and selects and develops control activities to address each risk. Management also considers a mix of transaction control activities and business performance reviews. In its selection and development of control activities, management considers the likelihood that a control might fail to operate effectively. In assessing the risk of failure, management assesses various factors, which may include:

- The type of control and frequency/complexity
- Risk of Management override
- Degree of judgment required to operate the control
- Changes/Competence of the personnel who perform the control
- Nature and materiality of misstatements that the control is intended to prevent/detect
- Degree control relies on the effectiveness of other controls
- Evidence of operation of the control from prior years

P10: Approach - Considering Alternative Control Activities to the Segregation of Duties

While resource or other constraints compromise the ability to appropriately segregate duties, management considers alternative control activities, such as timely periodic management reviews of reports that are prepared in sufficient detail for misstatements to be identified.
P10: Approach - Identifying Incompatible Functions

Using automated tools, organization charts, process flowcharts, or other means by which activities are documented, management identifies incompatibilities in functions that are needed to appropriately segregate duties. These incompatible functions are considered when developing or revising the policies for granting access to assets and systems. The policies are regularly updated to reflect changing responsibilities and activities.

Control Activities: Principle #11

The organization selects and develops general control activities over technology to support the achievement of objectives.

[NOTE: Full-Day Course available on GC’s]
Principle #11: Approaches

1. Using Risk and Control Matrices to Document Technology Dependencies
2. Evaluating End-User Computing
3. Implementing or Assessing Control Activities when Outsourcing IT Functions to a Third Party
4. Configuring the IT Infrastructure to Support Restricted Access and Segregation of Duties
5. Configuring IT to Support the Complete, Accurate, and Valid Processing of Transactions and Data
6. Administering Security and Access
7. Applying a SDLC over Packaged Software
8. Applying an SDLC over Software Developed in-House

P11: Approach - Using Risk and Control Matrices to Document Technology Dependencies

- Management documents the underlying technology that supports control activities in risk and control matrices, flow charts, or narratives. Using this information, management can document the linkage between control activities and technology.
- Management should understand which aspects of technology are important to the continued, proper operation of the technology and any associated automated controls. Management also develops an understanding of how various applications and technologies interface with each other.
P11: Approach - Evaluating End-User Computing (=SPREADSHEETS/DATABASES)

- Management understands the use of end-user computing, which includes spreadsheets, that supports its financially significant processes and associated control activities. Management assesses the risks of a misstatement resulting from an error in one of those end-user computing applications. Based on the level of risk, management selects and develops general control activities over the technology covering relevant processes over:
  - Technology Infrastructure
  - Security Management
  - End-user computing development and maintenance
  - Completeness and accuracy controls between the end-user computing system and other systems
- For high-risk end-user computing applications, management considers converting to an IT-supported application.

P11: Approach - Implementing or Assessing Control Activities when Outsourcing IT Functions to a Third Party

- Management outsources certain aspects of its IT infrastructure to an outside service provider, which may or may not have a "report on controls at a service organization/SOC 16" following an appropriate local or international standard.
- If a report is available, management uses it to determine what financially significant IT processes are covered, whether appropriate controls are in place at the service organization, and what controls are required in its own organization to mitigate risks to external financial reporting to an acceptable level.
P11: Approach - Configuring the IT Infrastructure to Support Restricted Access and Segregation of Duties

- The applications, databases, operating systems, and networks that support financially significant processes are configured to support restricted access to financial applications and data consistent with the organization’s policies and procedures.
- The configuration includes a means to authenticate users or systems and enforce restricted access, as well as key parameters, such as minimum password length and the aging of passwords.

P11: Approach - Configuring IT to Support the Complete, Accurate, and Valid Processing of Transactions and Data

- Management selects and develops control activities so that transaction processing, whether batch or real-time, is complete, accurate, and valid. Processing is actively checked for problems, either through a manual review of system status and logs or by automated programs with alarms. Timely corrective action is taken when problems are identified.
- Critical financial data and programs are regularly backed up and procedures are in place to completely and accurately do a restore. The restoration process is regularly tested to help ensure the backup and restoration processes work properly.
P11: Approach - Administering Security and Access

- Financial management establishes policies that define appropriate access rights to be consistent with job functions, including segregation of duties, for financially significant applications and processes. New access requests or changes to access are reviewed against the policy by the functional owner of the IT resource.

- The owner of the IT resource periodically recertifies access to ensure it is commensurate with policy. Problem reports, such as excessive improper logins, are regularly reviewed, and follow-up actions are taken when issues are identified.

P11: Approach - Applying a SDLC over Packaged Software

- Management considers many factors when selecting new packaged software, including functionality, application controls, security features, and data conversion requirements. Management utilizes component internal resources or hires a third-party vendor to implement the software, following the organization’s requirements.

- Management follows a defined change-control process to implement upgrades or patches. This includes assessing the nature of the upgrade or patch and whether it is appropriate to implement. If deemed appropriate, the patch or upgrade is system and user tested in an environment that mirrors production before being implemented.

- Key stakeholders, such as the functional users, finance, and IT, sign off on the change before implementation. Appropriate documentation is maintained to provide evidence that the changes have been made.
Managements follows a **full SDLC covering problem fixes to major implementations.** The SDLC covers a number of process steps and control activities, including the following:

- Initiation, Authorization, Tracking, and Analysis
- Design and Construction
- Testing and QA
- Data Conversation
- Program Implementation and Go-Live Authorization
- Documentation and Training

---

**Control Activities: Principle #12**

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

1. Developing & Documenting P&P
2. Deploying Control Activities through Business Unit or Functional Leaders
3. Conducting Regular and Ad Hoc Assessments of Control Activities

P12: Approach - Developing & Documenting P&P

Management develops and documents policies and procedures for all significant external financial reporting-related control activities. Procedures are documented using various formats, such as narratives, flowcharts, and control matrices. Management develops a standardized format for P&P, which may include:

- Reasons for the policy (risks to achievement of management's objectives)
- Locations, units and processes to which the policy and procedure applies
- Roles and responsibilities for owning, creating, implementing, executing, and maintaining the policy and procedure
- Matters covered by the P&P, including corrective action to be taken as part of performing the control activity
- Escalation procedures for policy exceptions
- Cross-references between associated P&P
- Required competency of personnel performing procedures
- Required timeframe for performing procedures
- Review date
### P12: Approach - Deploying Control Activities through Business Unit or Functional Leaders

- Business unit or functional leaders deploy control activities in their areas or responsibility by building the P&P into their organization’s day-to-day activities. In some cases, a centralized control function or team works with the business unit or functional leaders to help deploy P&P consistently across the organization. P&P are communicated in various ways, including running training programs, holding meetings, and distributing formal and informal documentation.

### P12: Approach - Conducting Regular and Ad Hoc Assessments of Control Activities

- On a regular basis, or when changes are made to financially significant processes and systems, control activity owners in conjunction with financial reporting and control experts review control activity documentation for continued relevance. Changes are made when redundant, obsolete, or ineffective control activities are found.
13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

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

15. The organization communicates with external parties regarding matters affecting the functioning of internal control.
Information & Communication: Principle #13

The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

Principle #13: Approaches

1. Creating an Inventory of Information Requirements
2. Obtaining Information from External Sources
3. Obtaining Information from Non-Finance Management
4. Creating and Maintaining Information Repositories
5. Using an Application to Process Data into Information
6. Enhancing Information Quality through a Data Governance Program
7. Identifying, Securing, and Retaining Financial Data and Information
P13: Approach - Creating an Inventory of Information Requirements

- Extensive information is available to management and comes from a wide variety of sources. For information to be relevant, it must be directly aligned to management’s needs and responsibilities for overseeing external financial reporting and monitoring the internal control system. A process for identifying information requirements and building an inventory enables management to focus attention on information that directly supports its needs.

- To achieve this, financial management defines common categories and types of information that are aligned to external financial reporting objectives and related risks as specified by management. From these categories, financial management identifies relevant information from both internal and external sources that are best suited to management’s needs. Financial management creates an inventory of information and maps each item to one or more members of management that have a role in external financial reporting.

P13: Approach - Obtaining Information from External Sources

- Finance personnel often rely on publications, events, and other information from external parties to gather information relevant to performing their responsibilities. The sources of data and information vary depending on the specific role and responsibilities of the individual. Sources of information may include:
  - Subscriptions to industry publications and regulatory updates
  - Participation in industry conferences, trade shows, and other events
  - Regular communications, both verbal and electronic, with suppliers, customers, or third-party service providers
  - Membership and participation in relevant organizations
  - Subscription to third-party mailing lists and social media feeds that pertain to the industry and company
  - Industry research reports
  - Peer industry calls and financial filings

- Finance personnel evaluate the external information gathered and incorporate significant events, trends, and changes into their day-to-day financial reporting or related internal control responsibilities.
P13: Approach - Obtaining Information from Non-Finance Management

- External financial reporting objectives are impacted by non-financial activities that occur throughout the business, information about new events, changes, or significant trends is needed to support accounting, disclosure, and internal control activities. Therefore, senior accounting and finance personnel meet at least monthly with management and personnel in other areas of the business — such as operations, human resources, compliance, and product development. During these meetings, information is gathered verbally and in writing on business events and trends. Topics may include:
  - New or lost significant customers, suppliers, or other stakeholders
  - Rate and impact of employee turnover
  - Unexpected trends, whether negative or positive
  - Indications of unethical or improper behavior
  - Budget versus actual and forecast expectations
  - Contractual, compliance, or regulatory issues
  - Customer or supplier complaints
  - Findings from internal audit reports

P13: Approach - Creating and Maintaining Information Repositories

- Senior management establishes a policy for handling information that is gathered, produced, and shared throughout the company. The policy is designed to facilitate the efficient capture, use, and reuse of relevant information supplied to management and personnel across the company.

- Management and employees in external financial reporting roles follow procedures for identifying and categorizing information. These procedures require that attributes about each piece of information be recorded before the information is accepted into the repository. The attributes may include:
  - Information Owner
  - Expected users
  - Sources (including systems and people)
  - Criticality
  - Frequency
  - Process Supported
  - Retention Period
P13: Approach - Using an Application to Process Data into Information

- Management designs its computer applications to capture data from internal and external sources, transform the data into information, and maintain the quality of data and information throughout processing and reporting. The activities relating to capturing and processing data about financial transactions are documented in company policies and procedures manuals. The application design includes automated application controls such as input checks for existence and validity and output checks for completeness and accuracy. It also is supported by technology general controls.

P13: Approach - Enhancing Information Quality through a Data Governance Program

- Senior management establishes a data governance program to support the company's objectives of ensuring reliability of information used in support of internal controls and external financial reporting. Senior management formalizes policies, procedures, and responsibilities for data and information management considering the volume, complexity, and demand for rapid capture and dissemination from multiple sources. The data governance program includes policies and procedures for:
  - Assigning roles and responsibilities between a central data management group, business functions, and IT
  - Validating sources of information
  - Establishing data-quality requirements before accepting sources into the information system
  - Accessing rights to underlying data and related information produced through processing
  - Protecting data during transmission and storage
P13: Approach - Identifying, Securing, and Retaining Financial Data and Information

- Senior IT management establishes policies to define categories of data and assign requirements for securing and retaining the data. These policies support management and employee responsibilities for securing information from unauthorized access or change and for adhering to retention and data destruction requirements.
- The senior data administrator develops processes and repositories to carry out the data classification policy. Data classification requirements are communicated to personnel responsible for transaction processing through periodic reminders on important internal control responsibilities.

Information & Communication: Principle #14

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

1. Communicating Information Regarding External Financial Reporting Objectives and Internal Control
2. Communicating Internal Control Responsibilities
3. Developing Guidelines for Communication to the Board of Directors
4. Reviewing Financial & Internal Control Information with the BoD
5. Communicating a Whistle-Blower Program to Company Personnel
6. Communicating through Alternative Reporting Channels
7. Establishing a Mentoring Program to Encourage Communicating with Management

P14: Approach - Communicating Information Regarding External Financial Reporting Objectives and Internal Control

- Senior management communicates information about the company’s financial reporting objectives, financial control requirements, and internal control policies and procedures, and how they support individual responsibilities through a variety of communication channels. The method of communication varies depending on the audience; the nature of the information, time sensitivity, cost, legal, or regulatory requirements and ability to use technology solutions. Mechanisms may include:
  - Department vision and mission objectives
  - Accounting and finance internal meetings or conferences to discuss internal control policies and procedures
  - Periodic employee surveys related to awareness and compliance to internal control policies and procedures
  - An Intranet site specific to internal control matters, including code of conduct, roles and responsibilities, policies, procedures, and other relevant matters
  - Regular organization-wide emails, newsletters, conference calls, webcasts, or meetings about updates no internal control matters
  - Senior finance and executive management visits to plants, sales offices, major customers, and other locations
P14: Approach - Communicating Internal Control Responsibilities

- Documentation on internal controls related to financially significant business processes and systems is stored in a shared repository that is accessible to management and personnel who are responsible for external financial reporting. This repository contains:
  - Risk assessment documentation
  - Business process documentation, including process flow diagrams and supporting narratives
  - Internal controls identified by management based on risk assessments
  - List of individual internal controls, including assignment responsibility for performance and review/approval to specified employees and management

- The internal audit department reviews the information in the repository as part of its ongoing and separate evaluations. Updates to specific internal controls are communicated to both the control performer and reviewer through email alerts with links to the repository.

P14: Approach - Developing Guidelines for Communication to the Board of Directors

- The Board of Directors establishes a board charter that defines the guidelines for information to be shared with the board of directors, responsibilities for communication, and the method of communication.

- The charter specifies key guidelines, which may include:
  - Frequency and number of meetings, including committees of the board
  - Objectives of each board of committee meeting
  - Nature and extent of information to be shared for each meeting
  - Responsibility for preparing and approving minutes
P14: Approach - Reviewing Financial & Internal Control Information with the BoD

- At designated board meetings, the CFO and supporting personnel present financial information, provide an analysis of the results compared with expectations, give updates on forecasts and major changes to original budgets, and communicate other matters of significance to financial reporting.
- On a regular basis, the CEO, CFO, and CAE present the draft external financial statements. Material events, changes in significant estimates, or assumptions and significant new disclosure matters since the prior quarter are also presented and discussed. The external auditors attend these meetings to present their point of view on the financial statements.
- At each quarterly meeting, the CFO and the CAE present a summary of key changes in internal control, results of evaluations, and actions in response to any deviations identified. Matters of significant are reported in writing. The audit committee holds separate private sessions with management and the external auditors.

P14: Approach - Communicating a Whistle-Blower Program to Company Personnel

- Management and the board establish a whistle-blower program for employees to use a hotline to communicate concerns, instances of perceived misconduct, matters relating to external financial reporting, or other significant matters that may impact internal control. To enhance employee awareness of the program, a number of communication channels are used. These include postings in high-traffic areas in offices and periodic messages from the director of human resources.
- The program allows employees who report matters through the hotline to remain anonymous, and all communication is completely confidential. Reported matters are evaluated by an objective party and communicated to the board of directors or, where appropriate, a specified delegate.
P14: Approach - Communicating through Alternative Reporting Channels

- Management provides an alternative to reporting to a line manager so that employees are confident that they will be heard. Alternative reporting and communications channels may include:
  - Mentoring programs to provide employees with a support structure beyond the direct line manager
  - Town hall meetings where employees are encouraged to ask questions and discuss their concerns
  - A staff council comprising of employees from various departments and various levels below manager which meet to discuss various issues and relays comments and observations to management.

P14: Approach - Establishing a Mentoring Program to Encourage Communicating with Management

- Management from all departments develop cross-functional and departmental communication processes and forums that enable personnel to communicate internal control matters across the entity. Representatives from each department have defined roles and responsibilities for communicating internal control matters using these processes and forums. The group meets periodically to discuss issues, trends, and upcoming events that impact internal controls.
- Control matters and issues noted by a shared service center, business unit, or department are communicated to other departments and business units. Management and personnel in the departments and business units evaluate and respond to the impact of these matters and issues.
Information & Communication: Principle #15

The organization communicates with external parties regarding matters affecting the functioning of internal control.

Principle #15: Approaches

1. Communicating Information to Relevant External Parties
2. Obtaining Information from Outside Sources
3. Surveying External Parties
4. Communicating the Whistle-Blower Program to Outside Parties
5. Reviewing External Audit Communications
P15: Approach - Communicating Information to Relevant External Parties

- Management considers all relevant external parties who have an interest in or who would be reasonably expected to obtain information about the company’s internal control over external financial reporting. The company’s disclosure committee has established a process to evaluate ongoing company events, policies, activities, and other matters that impact external parties that are important to the company’s external financial reporting objectives. The disclosure committee determines the information that should be reported to external parties, as needed. Such information may include:
  - Internal controls over transactions and balances that represent significant payables, receivables, or commitments to external stakeholders
  - Results of procedures for monitoring compliance with contractual commitments and related loss or damage provisions
  - Policies for protecting information received from external parties during normal business transactions
  - Customer responsibilities for managing their employees’ access to the company’s web-based ordering system to prevent unauthorized orders
  - Policies related to performing background checks and credit checks, or using collection agencies

P15: Approach - Obtaining Information from Outside Sources

- Management and other personnel stay abreast of new matters relevant to their area of responsibility in order to identify and respond to changes that may impact, directly or indirectly, external financial reporting objectives or the related internal control. Sources of information may include:
  - Publications that provide updates to financial accounting, reporting, and disclosure standards or regulations
  - Technical journals that analyze the impact of financial accounting and reporting matters
  - Competitor or peer regulatory filings
  - Information gathered at industry or trade association meetings
  - Industry, market, economic, or competitor data relevant to key metrics or accounting estimates
  - Alerts from outside counsel on regulatory or legal changes
  - Periodic meetings with external auditors and advisors to understand new accounting and disclosure requirements
  - Meetings with outside advisors or subject matter specialists with the expertise to assess complex accounting and disclosures for major transactions or events
  - Standard-setter and regulator projects and publications
  - Postings on organization-sponsored or supported social media websites or communication tools
P15: Approach - Surveying External Parties

- Management surveys customers, vendors, and others on their perception of the integrity and ethical values of company personnel. This survey process is controlled by company personnel independent of the main customer/vendor contacts.
- Management carries out surveys of external parties in a variety of ways, which may include:
  - Sending to all customers periodic surveys with standard questions regarding the company and its products and services
  - Providing a feedback mechanism on the customer’s website or through a feedback box on documents that are sent regularly to external parties
  - Periodically meeting with external parties, in person or by video or teleconference

P15: Approach - Communicating the Whistle-Blower Program to Outside Parties

- Management provides a whistle-blower phone number or email address to customers, suppliers, outsourcing companies, and other external parties to facilitate feedback on potential improprieties or improper or unreliable financial reporting. The contact information is disseminated through various means, such as the company’s website and on invoices sent to customers.
Following the external auditor’s review of financial information and independent evaluation of internal control effectiveness, management receives a written summary of significant matters identified during the course of the work. The BoD discusses these at a subsequent meeting, where external audit personnel discuss their findings and management discusses proposed resolutions.
Monitoring Activities

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
Monitoring Activities: Principle #16

The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
Principle #16: Approaches

1. Periodically Reviewing the Mix of Monitoring Activities
2. Designing and Implementing a Dashboard
3. Using Technology to Support Monitoring Activities
4. Conducting Separate Evaluations
5. Using Internal Audit to Conduct Separate Evaluations
6. Understanding Controls at an Outsourced Service Provider

P16: Approach - Periodically Reviewing the Mix of Monitoring Activities

- Senior management meets periodically to review the allocation of effort between ongoing evaluations and separate evaluations used to conduct monitoring activities. The mix of planned monitoring activities over internal control of external financial reporting may depend on senior management’s assessment of:
  - The entity’s regulatory requirements and financial reporting objectives
  - How quickly the entity’s industry and/or regulatory environment is changing or anticipated to change
  - The results of historical evaluations of control effectiveness
  - The extent of ongoing monitoring within the associated processes
  - Changes that have occurred in the current year that impact other components of internal control
- Senior management may also increase the frequency of separate evaluations from the initial plan in processes where:
  - Existing monitoring activities raise potential deficiencies in the system of internal control
  - Key performance indicators, which correlate to surfacing potential deficiencies in internal control, have exceeded a prescribed threshold
### P16: Approach - Designing and Implementing a Dashboard

- As part of its ongoing evaluations, management develops and implements dashboards for reviewers to use in the ordinary course of business. Reviewers are usually supervisors of those employees with first-level knowledge and who are accountable for processes, activities, and their controls. Dashboards may include:
  - Detailed and/or summarized information about control performance
  - Metrics being measured and/or information being highlighted for evaluation and investigative follow-up
  - Visual depictions of the status of control operation
  - Details of status including frequency of assessment and last assessment
  - Known current deficiencies and their remediation status
  - Key personnel and contract details for those responsible for processes and sub-processes

### P16: Approach - Using Technology to Support Monitoring Activities

- Management uses technology to support the monitoring of the system of internal controls in the ordinary course of business through automated monitoring applications. Management uses the automated monitoring application to efficiently and continuously review large volumes of data at a low cost with a high standard of objectivity. Automated monitoring activities may include:
  - Checking transactions against predefined thresholds for anomalies
  - Monitoring transactions for trends or patterns
  - Assessing automated performance indicators, metrics, and measures that may lead to improvements in process and business
Management may conduct separate evaluations of internal controls over external financial reporting by:

- Conducting ad hoc supervisory management visits and reviews
- Conducting cross-operating unit reviews using management from similar operating units within the company
- Comparing components of internal control with another similar entity by benchmarking or using a peer evaluation
- Developing a self-assessment questionnaire for a business process for use by personnel responsible for the controls within a particular business unit or function
- Hiring an independent third party to perform specific evaluation

Management uses an appropriately staffed and adequately trained internal audit function to provide an objective perspective on key elements of the internal control over external financial reporting. Internal audit reports are distributed to senior management, the BoD, and others who are positioned to act on the report’s recommendations. Internal audit’s separate evaluations may be influenced by:

- The entity’s regulatory environment and management’s methodology and plans for achieving compliance with its financial reporting objective
- An understanding, independent of management, of how the internal control system addresses meaningful risks
- Approval for the planned separate evaluation activities by the BoD or one of its committees.
P16: Approach - Understanding Controls at an Outsourced Service Provider

- Management obtains and reviews periodic information from outsourced service providers to detect any changes in the activities that impact the entity’s system of internal control over external financial reporting. Information obtained may include:
  - The outsourced service provider’s applicable control objectives
  - Details about which of the outsourced service provider’s internal control has been examined and included in any report
- To determine what impact any identified changes may have on the entity’s system of internal control over external financial reporting, the following may also be assessed:
  - Whether management appropriately considered known changes in business processes and their impact on internal control, and whether they were communicated to the outsourced service provider, since such changes could impact the entity’s control objectives and design
  - Whether the exceptions were noted that may trigger further review by senior management
  - Whether management is satisfied with the independence and objectivity of the report

Monitoring Activities: Principle #17

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

1. Assessing and Reporting Deficiencies
2. Monitoring Corrective Action
3. Developing Guidelines for Reporting Deficiencies

P17: Approach - Assessing and Reporting Deficiencies

- Management develops P&P to periodically assess and communicate deficiencies that result from the entity’s monitoring activities and other sources. Management establishes a practice where all deficiencies in internal control over external financial reporting, regardless of materiality, are reported to the responsible manager and at least one level of management above, both of whom are positioned to take reporting to senior management or the board based on criteria established by standard setters or regulators. The criteria should include the following:
  - Nature of the deficiency
  - Source of the deficiency
  - Known magnitude of a misstatement caused by the deficiency to the entity’s financial statements
  - The likelihood and potential magnitude of a misstatement caused by the deficiency to the entity’s financial statements
  - An aggregation of deficiencies affecting similar areas that could indicate a more serious deficiency
P17: Approach - Monitoring Corrective Action

- Management establishes a practice to review the status of corrective actions taken to verify that reported deficiencies are remediated in a timely manner. The corrective action practice may include:
  - Regularly scheduled meetings to review the status of corrective actions
  - An established electronic or hard-copy report in which corrective actions are summarized and collected
  - Delegated oversight to a responsible party, such as an internal audit function

P17: Approach - Developing Guidelines for Reporting Deficiencies

- The BoD develops a shared expectation with senior management on the types of control deficiencies that get reported to the board. The BoD understands the facts and circumstances regarding internal control deficiencies that impact external financial reporting and provides oversight on management’s conclusions and remediation plans.
Transition & Impact

- Users are encouraged to transition applications and related documentation to the updated Framework as soon as feasible
- Updated Framework will supersede original Framework at the end of the transition period (i.e., December 15, 2014)
- During the transition period, external reporting should disclose whether the original or updated version of the Framework was used
- Impact of adopting the updated Framework will vary by organization
  - Does your system of internal control need to address changes in business?
  - Does your system of internal control need to be updated to address all principles?
  - Does your organization apply and interpret the original framework in the same manner as COSO?
  - Is your organization considering new opportunities to apply internal control to cover additional objectives?

Transition & Impact (Continued)

- The principles-based approach provides flexibility in applying the Framework to multiple, overlapping objectives across the entity
  - Easier to see what is covered and what is missing
  - Focus on principles may reduce likelihood of considering something that’s irrelevant
- Understanding the importance of specifying suitable objectives focuses on those risks and controls most important to achieving these objectives
- Focusing on areas of risk that exceed acceptance levels or need to be managed across the entity may reduce efforts spent mitigating risks in areas of lesser significance
- Coordinating efforts for identifying and assessing risks across multiple, overlapping objectives may reduce the number of discrete risks assessed and mitigated
Transition & Impact (Continued)

- Selecting, developing, and deploying controls to effect multiple principles may also reduce the number of discrete, layered-on controls.
- Applying an integrated approach to internal control - encompassing operations, reporting, and compliance – may lessen complexity.
- In assessing severity of internal control deficiencies, use only the relevant classification criteria as set out in the Framework or by regulators, standard-setting bodies, and other relevant third parties, as appropriate.

Copyright © 2013 COSO/ Sunera LLC

SECTION SOURCE: IIA.ORG

2012 IIA Standards Update

SECTION SOURCE: IIA.ORG
Session Overview

- Why the *Standards* matter
- The key changes in 2012
- Best practices for implementation

Standards – Why do they Matter?
Overview of the IIA Standards

Attribute Standards:
- Purpose, Authority and Responsibility .................................................. (1000)
- Independence and Objectivity ................................................................. (1100)
- Proficiency and Due Professional Care ...................................................... (1200)
- Quality Assurance and Improvement Program ......................................... (1300)

Performance Standards:
- Managing the Internal Auditing Activity ............................................... (2000)
- Nature of Work ......................................................................................... (2100)
- Engagement Planning ............................................................................ (2200)
- Performing the Engagement ................................................................. (2300)
- Communicating Results ........................................................................ (2400)
- Monitoring Progress ............................................................................. (2500)
- Communicating the Acceptance of Risks ................................................ (2600)

Standards are Critical

- Delineate basic principles that represent the practice of internal auditing
- Framework for performing and promoting a broad range of value-added internal auditing
- Establish the basis for the evaluation of internal audit performance
- Foster improved organizational processes and operations
Key Changes in 2012

Why Change?

- The *Standards* must remain current, relevant, and timely for the profession
- The IPPF process requires that the Standards be reviewed at least once every three years
- Ongoing changes are a key component of the continued development of the IPPF
Summary of the Changes

- Clarify responsibilities for conforming with the *Standards*
- Increased focus on Quality Assurance & Improvement
- Clarify the CAE’s role to communicate unacceptable risk
- Explicitly require timely audit plan adjustments
- Emphasize coverage of risks to strategic objectives
- Changes to Glossary Terms

Responsibilities for Conformance

Adding the following wording to the Introduction of the *Standards*:

The *Standards* apply to individual internal auditors and internal audit activities. All internal auditors are accountable for conforming with the Standards related to individual objectivity, proficiency, and due professional care. In addition, internal auditors are accountable for conforming with the Standards, which are relevant to the performance of their job responsibilities. Chief audit executives are accountable for overall conformance with the Standards.

<table>
<thead>
<tr>
<th>Exposure Results:</th>
<th>Yes: 87%, No: 4.1%, No Opinion: 5.8%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standards Board Decision:</td>
<td>Adopt the exposed change</td>
</tr>
</tbody>
</table>
Organizational Independence

**1110 - Organizational Independence**
The chief audit executive must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities. The chief audit executive must confirm to the board, at least annually, the organizational independence of the internal audit activity.

**Interpretation:**
Organizational independence is effectively achieved when the chief audit executive reports functionally to the board. Examples of functional reporting to the board involve the board:

- Approving the internal audit charter;
- Approving the risk based internal audit plan;
- Approving the internal audit budget and resource plan;
- Receiving communications from the chief audit executive on the internal audit activity’s performance relative to its plan and other matters;
- Approving decisions regarding the appointment and removal of the chief audit executive;
- Approving the remuneration of the chief audit executive; and
- Making appropriate inquiries of management and the chief audit executive to determine whether there are inappropriate scope or resource limitations.

**Exposure Results:** Yes: 85%, No: 9.8%, No Opinion: 5.3%

**Standards Board Decision:** Adopt the exposed change

---

**Standard 1110 – Best Practices**

- Board or audit committee approve the risk assessment and related audit plans
- Private meetings with the CAE and audit committee / board chair
- Frequent interactions with board outside formal board meetings
Increased Focus – Quality Assurance

1312 - External Assessments
External assessments must be conducted at least once every five years by a qualified, independent reviewer assessor or review assessment team from outside the organization. The chief audit executive must discuss with the board:

- The need for more frequent form and frequency of external assessments; and
- The qualifications and independence of the external reviewer assessor or review assessment team, including any potential conflict of interest.

Interpretation: 
*External assessments can be in the form of a full external assessment, or a self-assessment with independent external validation.*

<table>
<thead>
<tr>
<th>Exposure Results</th>
<th>Yes: 86.5%, No: 7.6%, No Opinion: 5.9%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standards Board Decision</td>
<td>Modify the exposed change</td>
</tr>
</tbody>
</table>

Standard 1312 – Best Practices

- Proactive internal quality assessment and improvement program

- Fully embrace the spirit and the letter of the external quality Standards

- Have practices to allow execution and delivery of quality work

- Leverage the external quality assessment to promote internal audit by including a statement of conformance in each audit report
Timely Audit Plan Adjustments

2010 – Planning
The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization’s goals.

Interpretation:
The chief audit executive is responsible for developing a risk-based plan. The chief audit executive takes into account the organization’s risk management framework, including using risk appetite levels set by management for the different activities or parts of the organization. If a framework does not exist, the chief audit executive uses his/her own judgment of risks after consultation with senior management and the board. The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organization’s business, risks, operations, programs, systems, and controls.

Exposure Results: Yes: 92.5%, No: 4.3%, No Opinion: 3.2%
Standards Board Decision: Adopt the exposed change

Standard 2010 – Best Practices

- Identify and consider stakeholder input into the internal audit risk assessment process
- Don’t let major risks go uncovered; find a way to address them before they get too big
- Educate key stakeholders on important areas of risk and on actions needed to address issues
- Develop an ongoing communications process with management to keep current on changing business and risk issues
Inclusion of Strategic Risk

2120.A1
The internal audit activity must evaluate risk exposures relating to the organization’s governance, operations, and information systems regarding the:

- Achievement of the organization’s strategic objectives;
- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations and programs;
- Safeguarding of assets; and
- Compliance with laws, regulations, policies, procedures, and contracts.

Exposure Results: Yes: 90.6%, No: 5.9%, No Opinion: 3.5%
Standards Board Decision: Adopt the exposed change

Inclusion of Strategic Risk

2130.A1
The internal audit activity must evaluate the adequacy and effectiveness of controls responding to risks within the organization’s governance, operations, and information systems regarding the:

- Achievement of the organization’s strategic objectives;
- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations and programs;
- Safeguarding of assets; and
- Compliance with laws, regulations, policies, procedures, and contracts.

Exposure Results: Yes: 90.9%, No: 5.7%, No Opinion: 3.4%
Standards Board Decision: Adopt the exposed change

- Internal audit involvement in key strategic initiatives
- A “seat at the table”
- Address the organizations key strategic risks
- Serve on IT development teams

Disseminating Results

2440 – Disseminating Results
The chief audit executive must communicate results to the appropriate parties.

Interpretation:
The chief audit executive or designee reviews and approves the final engagement communication before issuance and decides for deciding to whom and how it will be disseminated. When the chief audit executive delegates these duties, he or she retains overall responsibility.

Exposure Results: Yes: 84.7%, No: 11.8%, No Opinion: 3.5%
Standards Board Decision: Modify the exposed change
Standard 2440 – Best Practices

- Communicate with impact
- Develop an ongoing communications process with management to keep current on changing business and risk issues
- Develop systemic and trending information that would be valued by stakeholders
- Ensure management is attentive to audit issues and that top management and the audit committee are kept aware of management’s corrective actions

Acceptance of Risk

2600 – Resolution of Senior Management’s Communicating the Acceptance of Risks

When the chief audit executive believes concludes that senior management has accepted a level of residual risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the decision regarding residual risk is chief audit executive determines that the matter has not been resolved, the chief audit executive must report communicate the matter to the board for resolution.

Interpretation:
The identification of risk accepted by management may be observed through an assurance or consulting engagement, monitoring progress on actions taken by management as a result of prior engagements, or other means. It is not the responsibility of the chief audit executive to resolve the risk.

Exposure Results: Yes: 89%, No: 7%, No Opinion: 4%

Standards Board Decision: Adopt the exposed change
Standard 2600 – Best Practices

- When you believe the organization is facing unacceptable risk or certain actions are just not right, speak out.
- Use good judgment on what are real issues, but make it clear that internal auditing has a voice and is willing to use it.

Clarify the Definition of “Board”

Board –
A board is an organization’s governing body, such as a board of directors, supervisory board, head of an agency or legislative body, board of governors or trustees of a non-profit organization, or any other designated body of the organization, including the audit committee to whom the chief audit executive may functionally report.

The highest level of governing body charged with the responsibility to direct and/or oversee the activities and management of the organization. Typically, this includes an independent group of directors [e.g., a board of directors, a supervisory board, or a board of governors or trustees]. If such a group does not exist, the “board” may refer to the head of the organization. “Board” may refer to an audit committee to which the governing body has delegated certain functions.

Exposure Results: Yes: 88%, No: 5.7%, No Opinion: 6.3%
Standards Board Decision: Modify the exposed change
New Definition of “Engagement Opinion”

**Engagement Opinion**

The rating, conclusion, and/or other description of results of an individual internal audit engagement, relating to those aspects within the objectives and scope of the engagement.

**Exposure Results:**
- Yes: 89.1%
- No: 4.8%
- No Opinion: 6.2%

**Standards Board Decision:** Modify the exposed change

---

New Definition of “Overall Opinion”

**Overall Opinion**

The overall ratings, conclusions, or other descriptions of results provided by the chief audit executive addressing, at a broad level, governance, risk management and control processes of the organization. An overall opinion is based on the results of a number of individual engagements and other activities for a specific time interval.

**Exposure Results:**
- Yes: 88.2%
- No: 5.4%
- No Opinion: 6.5%

**Standards Board Decision:** Modify the exposed change
Other Changes

- 1311 – Internal Assessment
- 1320 – Reporting on the Quality Assurance and Improvement Program
- 2201 – Plan Consideration
- 2220 – Engagement Scope
- 2210.A3
- Control Processes
- Delete the definition of “residual risk”
- Keep the current definition of “risk”

Fraud Risk Assessment
The Definition of Fraud

“... any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.”

Categories of Fraud Risk

- **Misappropriation of Assets**
  - involve the theft or misuse of an organization’s assets. (Common examples include skimming revenues, stealing inventory, and payroll fraud.)

- **Corruption**
  - fraudsters wrongfully use their influence in a business transaction in order to procure some benefit for themselves or another person, contrary to their duty to their employer or the rights of another. (Common examples include accepting kickbacks and engaging in conflicts of interest.)

- **Fraudulent Financial Statements**
  - falsification of an organization’s financial statements. (Common examples include overstating revenues and understating liabilities or expenses.)
### Asset Misappropriation

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payroll</td>
<td>• Payment to fictitious employees</td>
</tr>
<tr>
<td></td>
<td>• Payment to terminated employees</td>
</tr>
<tr>
<td></td>
<td>• Overpayment to existing employees</td>
</tr>
<tr>
<td>Inventory</td>
<td>• Theft of inventory items</td>
</tr>
<tr>
<td></td>
<td>• Consistent shrinkage of items</td>
</tr>
<tr>
<td></td>
<td>• Increased defective/warranty claims</td>
</tr>
<tr>
<td>Credit Cards</td>
<td>• Reimbursement for personal expenses</td>
</tr>
<tr>
<td></td>
<td>• Use of card to circumvent competitive bid requirements</td>
</tr>
<tr>
<td>Larceny</td>
<td>• Theft of materials, supplies, cash</td>
</tr>
<tr>
<td>Purchasing</td>
<td>• Using purchasing authority to purchase raw materials for personal use.</td>
</tr>
<tr>
<td>Procurement</td>
<td>• Using procurement card for personal, exorbitant purchases</td>
</tr>
<tr>
<td>Reimbursement</td>
<td>• Reimbursement for undocumented expenses</td>
</tr>
<tr>
<td></td>
<td>• Reimbursement for luxury accommodations</td>
</tr>
<tr>
<td></td>
<td>• Reimbursement for travel expenses of family members</td>
</tr>
<tr>
<td>Improper Payments</td>
<td>• Payments to phantom vendors, shell companies</td>
</tr>
</tbody>
</table>

### Corruption/FCPA

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fictitious Revenue</td>
<td>• Improper or early revenue recognition</td>
</tr>
<tr>
<td></td>
<td>• Falsifying revenue</td>
</tr>
<tr>
<td></td>
<td>• Earnings manipulation through reserves</td>
</tr>
<tr>
<td></td>
<td>• Recording pending transactions as completed transactions</td>
</tr>
<tr>
<td>Overstating Assets</td>
<td>Improper valuation of securities, inventory, fixed assets</td>
</tr>
<tr>
<td>Understating Liabilities</td>
<td>• Hiding losses in future reporting periods</td>
</tr>
<tr>
<td>and Expenses</td>
<td>• Understating expense account balances</td>
</tr>
<tr>
<td></td>
<td>• Reclassifying (capitalizing) expenses as assets</td>
</tr>
<tr>
<td></td>
<td>• Improper valuation or manipulation of intercompany accounts</td>
</tr>
<tr>
<td>Improper Note Disclosure</td>
<td>• Omission of contingencies or subsequent events</td>
</tr>
<tr>
<td>Non-financial</td>
<td>• Falsifying external documents to suppliers</td>
</tr>
<tr>
<td></td>
<td>• Internal memorandums give misleading information</td>
</tr>
<tr>
<td></td>
<td>• Publicly announced unsubstantiated information</td>
</tr>
<tr>
<td>Management Estimates</td>
<td>• Manipulation of management estimates for receivables, goodwill or depreciation</td>
</tr>
</tbody>
</table>
## Financial Statement Fraud

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Scenario</th>
</tr>
</thead>
</table>
| Fictitious Revenue  | • Improper or early revenue recognition  
• Falsifying revenue  
• Earnings manipulation through reserves  
• Recording pending transactions as completed transactions |
| Overstating Assets  | • Improper valuation of securities, inventory, fixed assets                                   |
| Understating Liabilities and Expenses | • Hiding losses in future reporting periods  
• Understating expense account balances  
• Reclassifying (capitalizing) expenses as assets  
• Improper valuation or manipulation of intercompany accounts |
| Improper Note Disclosure | • Omission of material contingencies or subsequent events                                      |
| Non-financial       | • Falsifying external documents to suppliers  
• Internal memorandums give misleading information  
• Publicly announced unsubstantiated information |
| Management Estimates | • Manipulation of management estimates for receivables, goodwill or depreciation               |

### Fraud Risk Assessment

![Fraud Risk Assessment](attachment:image)
What is Risk?

- “The degree of probability that an unfavorable event will significantly impact a functional area’s ability to meet the organization’s objectives”

FRA - Purpose

- Identify and recognize fraud risks in the organization
- Determine the likelihood
- Determine how to manage and mitigate fraud risk
- Determine critical information
- Identify systems that process, store, or transmit critical information used for red flag identification
- Discover vulnerabilities
- Create new processes, controls and procedures for mitigating fraud risk
All fraud risks are identified and assigned a risk rating

Who Should be Involved?

- C – Suite Officer
  - CEO
  - CFO
  - CIO
  - General Counsel
  - Chief Compliance Officer
- Management
  - Business Unit Managers
  - Sales
  - Marketing
  - Human Resources
- Accounting
  - Controller
  - Accounting Manager
  - Accounting Supervisors
- Oversight
  - Internal Audit
  - Board of Directors
  - Audit Committee
  - External Auditors
Step 1 – Identify and Evaluate Fraud Risk Factors

1. Schedule interviews and develop the approach.
2. Identify fraud risk factors at the entity level, significant locations, accounts and business process level. **NOTE:** Consider whether each fraud risk factor indicates the existence of an incentive/pressure, opportunity or attitudes/rationalizations.
3. For each identified fraud risk factor, identify the account balances and potential errors that may be affected and assess the fraud risks.
Step 1 – Identify and Evaluate Fraud Risk Factors

**Pitfalls**
- Fraud Risk Factors are not considered
- Existing controls are considered
- The potential for management override of controls is not considered
- Interviews are not value-added

**Recommendations**
- Use the Fraud Triangle to explain the significance of fraud risk factors and to initiate thinking
- Do not consider controls EXCEPT when considering the potential for management override
- Develop interview approach that matches area and culture

---

Identify fraud risk factors at the entity level, significant location, significant account and business process level. Consider whether each fraud risk factor indicates the existence of incentive, pressure, opportunity or attitude and rationalization.

Identify incentives / pressures to commit fraud, opportunities to commit fraud, or attitudes / rationalizations to justify fraud.
- Personnel from various levels of the organization should be involved in the process.
- Consider internal and external (e.g., regulatory, industry) influences.
Step 2: Identify Possible Fraud Risks, Schemes and Scenarios

1. Identify fraud risks and determine if the fraud risks are pervasive or specific.
2. **Brainstorm** specific fraud schemes that could result from the specific risks identified.
3. For each fraud scheme, identify internal and external parties who could be involved with reference to incentives/pressure, opportunities, attitudes & rationalizations.

**Pitfalls**
- The schemes are too general, not allowing for sufficient consideration of risks and preventing appropriate level of mapping to controls
- The schemes do not consider the potential for management override of controls
- The schemes do not consider the potential for collusion
- **Brainstorming** ineffective

**Recommendations**
- Detail each scheme by considering:
  - Why?
  - Who?
  - What?
  - Where?
  - When?
  - How?
Step 3: Prioritize Identified Fraud Risks

- Evaluate possible fraud schemes by:
  - Type
  - Likelihood
  - Significance
  - Pervasiveness
- Consider Inherent Risk Rating (IRR)

![Likelihood/Magnitude Matrix](image)

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote</td>
<td>Low (&lt;$50K)</td>
<td>Low (&lt;$50K)</td>
<td>Med ($100K-$500K)</td>
<td>High (&gt;$100K)</td>
</tr>
<tr>
<td>Possible</td>
<td>Low (&lt;$50K)</td>
<td>Med ($100K-$500K)</td>
<td>High (&gt;$100K)</td>
<td>Critical (&gt;$500K-$100K)</td>
</tr>
<tr>
<td>Likely</td>
<td>Low (&lt;$50K)</td>
<td>Med ($100K-$500K)</td>
<td>High (&gt;$100K)</td>
<td>High</td>
</tr>
<tr>
<td>Expected</td>
<td>Low (&lt;$50K)</td>
<td>Med ($100K-$500K)</td>
<td>High (&gt;$100K)</td>
<td>High</td>
</tr>
</tbody>
</table>

Likelihood Criteria:
- Expected \(>90\%\)
- Likely \(50-90\%\)
- Possible \(20-50\%\)
- Remote \(<1\%\)
Step 4. Evaluate the Controls’ Existence and Effectiveness

1. Link fraud schemes to mitigating controls. Assess whether each mapped or linked control activity is preventative or detective in nature.
2. Evaluate the effectiveness of controls to determine if they sufficiently mitigate the risk of the identified fraud schemes (control gap analysis).
3. Evaluate the residual fraud risk.

---

Step 4. Evaluate Mitigating Controls

- Antifraud control activities can be preventative or detective in nature
  - Preventative controls are designed to mitigate specific fraud risks and can deter frauds from occurring
  - Detective control activities are designed to identify fraud if it occurs. Detective controls can also be used as a monitoring activity to assess the effectiveness of antifraud controls and may provide additional evidence of the effectiveness of antifraud programs and controls.
4. Evaluate Mitigating Controls

- Special consideration should be given to the risk of management override of controls.
- Some programs and controls that deal with management override include:
  - Active oversight from the audit committee
  - Whistle-blower programs and a system to receive and investigate anonymous complaints; and
  - Reviewing journal entries and other adjustments for evidence of possible material misstatement due to fraud.

4. Evaluate Mitigating Controls

**Pitfalls**
- Where gaps are identified, no remediation efforts are made
- Future changes in risk are not incorporated into the FRA and remediation is not performed
- Effectiveness of controls is not evaluated
- Mapping is done incorrectly and without consideration of existing controls and documentation

**Recommendations**
- Design and implement controls to close identified gaps
- The FRA should be iterative and should be reassessed at least annually and when there is a significant change in the control environment
- Evaluating the effectiveness of the controls
- Only map those controls identified as significant
- Identify entity level controls that will assist in mitigating remaining residual risk
- Leverage of existing efforts and controls
Control Risk Rating

- **Evaluate the Control Risk Rating** –
  - Determine if controls sufficiently mitigate the identified fraud risks and schemes
  - Decide whether existing controls should be improved or new controls are required
  - Consider both the design and the implementation of the control in mitigating the fraud risk

*Fraud controls can be tricky!*
*Consider possible management override of controls*

### 4. Control Risk Rating

<table>
<thead>
<tr>
<th>Sub Type</th>
<th>Type Detail</th>
<th>Fraud Schemes</th>
<th>Notes</th>
<th>Gross Risk Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gifts/Trav/Bribes</td>
<td>Employee Benefits</td>
<td>Kickbacks and/or bribes from third-party sources</td>
<td></td>
<td>High</td>
</tr>
<tr>
<td>Commission schemes</td>
<td>Refer to Documents</td>
<td>Manipulate data and/or change data (i.e., favor to value, doc type, purchase price, etc., to increase</td>
<td></td>
<td>Med</td>
</tr>
<tr>
<td>Loss of Information</td>
<td>Insider trading</td>
<td>Insider trading</td>
<td></td>
<td>High</td>
</tr>
<tr>
<td>Loss of Information</td>
<td>Misuse of confidential information</td>
<td>Borrower data information</td>
<td></td>
<td>High</td>
</tr>
</tbody>
</table>
Step 5: Risk Treatment

1. Prepare a Fraud Risk Action Plan to treat and mitigate fraud risk schemes requiring attention.

- Prepare a Fraud Risk Action Plan to treat and mitigate fraud risk schemes requiring attention.
  - Controls should be implemented or enhanced for identified fraud schemes where controls are not already present, inadequately designed or poorly implemented.
  - Ensure overall responsibility is assigned to responsible personnel to monitor control implementation as detailed in the Fraud Risk Action Plan.
  - This responsibility could be defined in the Fraud Control Policy of the entity or specified elsewhere.
  - The Audit Committee should oversee the entire process.
Documenting the FRA

- Documentation may include:
  - Spreadsheet listing identified risks, controls and evaluations
  - “Heat map” summary of key risks
  - Process narrative
  - Minutes of fraud brainstorm sessions
  - Copies of instructions and reference materials provided to Participants
  - E-mail and other correspondence related to the process
  - Minutes of audit committee meetings during which management’s fraud risk assessment was presented, reviewed, discussed, or approved

Monitoring the FRA – Keep it Current

- Conduct quarterly updates
- Imbed on-going FRA in 404 efforts
- Re-visit FRA as part of ERM activities
- Report changes and updates to Sr. Team and Board on a quarterly basis
- Update FRA for changes in the business and/or business environment (economy, industry, changes in competitor businesses)
- Use the FRA to refine and focus internal audit testing
### Conducting the FRA

<table>
<thead>
<tr>
<th>Step</th>
<th>Approach</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Identify &amp; Evaluate Fraud Risk Factors</td>
<td>Identify fraud risk factors and account balances and potential errors related to each fraud risk</td>
</tr>
<tr>
<td>2</td>
<td>Identify Possible Fraud Risks, Schemes &amp; Scenarios</td>
<td>Identify fraud risks and specific fraud schemes</td>
</tr>
<tr>
<td>3</td>
<td>Prioritize Identified Fraud Risks</td>
<td>Analyze the likelihood and significance of possible fraud schemes</td>
</tr>
<tr>
<td>4</td>
<td>Evaluate Whether Existing Controls Exist / Are Effective</td>
<td>Link fraud schemes to mitigating controls, evaluate control design and implementation, and evaluate residual risk of each fraud scheme</td>
</tr>
<tr>
<td>5</td>
<td>Risk Treatment</td>
<td>Prepare Fraud Risk Action Plan and implement plan</td>
</tr>
</tbody>
</table>

### Top Fraud Risk and Response

- Customize Response to Identified Fraud Schemes and Scenarios
<table>
<thead>
<tr>
<th>Process</th>
<th>Fraud Scheme</th>
<th>Response</th>
</tr>
</thead>
</table>
| 1. Revenue                          | Improper/early revenue recognition  
 Fictitious Revenue               | Implement month-end review of financial statements  
 Require review and approval of submitted forms                        |
| 2. Expenses                         | Hiding losses in future reporting periods                                   | Implement month-end review of financial statements                      |
| 3. Cash and Cash Equivalents        | Larceny  
 Defalcation                                                          | Establish ACH deposit into main operating account  
 Implement lockbox through independent bank                           |
| 4. Occupational Injury              | Non-compliance with FMLA, abuse of FMLA                                     | Require review and approval of submitted forms                        |
| 5. Financial Reporting              | Manipulation of management estimates for receivables, goodwill, or depreciation | Review and approval of journal entries;  
 Require supporting documentation for all estimates                   |
| 6. Improper Note Disclosure          | Omission of material contingencies                                           | Implement month-end checklist reviewed by various members of management |
| 7. Hiring Process                   | Payment to fictitious employees                                             | Segregation of duties in the payroll process;  
 outsource payroll                                                      |
| 8. Compliance with contracts        | Awarding contracts to parties related to individuals involved in the decision-making process | Involve various members of management in contract approval; require two signatures for approval of material contracts |
| 9. Assets                            | Improper valuation of securities, inventory, fixed assets                  | Management review and approval of valuation methods                    |
| 10. Expense reimbursement process    | Reimbursement for undocumented expenses                                    | Require employee expense reimbursement forms with attached original receipts |
| 11. Competitive Bid Rigging          | Establishing criteria that gives select vendors an unfair advantage        | Require independence confirmation for all members involved in negotiations |
| 12. Performance and Compensation Review | Overpayment to existing employees                                         | Segregation of duties in the payroll process;  
 outsource payroll                                                      |
| 13. Credit Card Process             | Reimbursement for personal, non-deductible expenses                        | Require employee acceptance of Terms of Use and re-payment for personal expenses |
| 14. Non-Financial                   | Falsifying external documents to suppliers                                 | Require approved contracts and purchase orders                        |
| 15. Document Storage                | Destruction or disappearance of records                                     | Establish Code of Conduct that restricts tampering with records; third party document records |
Questions?

Brian Amend  
Managing Partner  
bamend@sunera.com  
(972) 955-5652

Danny M. Goldberg  
Partner, Professional Development  
dgoldberg@sunera.com  
(214) 514-8883