In Control: Getting Familiar with the New COSO Guidelines

CSMFO

Monterey, California

February 18, 2015

Background on COSO

Part 1

Development of a comprehensive framework of internal control

Internal Control – Integrated Framework (1992)

Traditional view

- Poor internal control is the fault of management

Treadway Commission (1987)

- Treadway Commission on Fraudulent Financial Reporting
  - Sponsored by
    - American Accounting Association
    - American Institute of Certified Public Accountants
    - Financial Executives International
    - Institute of Management Accountants
    - The Institute of Internal Auditors

Critical reassessment

- *Internal control* needs to be defined
- Case needs to be made for management involvement
- Three responsible parties need to work together
  - Management
  - Governing body
  - Independent auditor

Cooperative effort for change

- The organizations that sponsored the Treadway Commission agree to work together to facilitate change
  - Council of Sponsoring Organizations = COSO
- Result of that effort
  - *Internal Control—An Integrated Framework* (1992)
    - "COSO Report" (COSO 1992)

Basic approach of COSO Report

- All entities share certain common objectives
- Internal control = means used to achieve
- To be successful, internal control must
  - Involve both the governing body and management
  - Be comprehensive

COSO definition

- 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:
  1. Effectiveness and efficiency of operations
  2. Reliability of financial reporting
  3. Compliance with applicable laws and regulations

Key concepts

- Process
  - Dynamic vs. static
  - Components interrelated
- Personnel
  - More than policies and procedures
- Reasonable assurance
  - Cost-benefit must be considered
- Achievement of objectives
  - Internal control logically derived from objectives
    - Source of consistency

Who is responsible?

- Management primarily responsible
  - Direct beneficiary
  - Uniquely positioned to establish and maintain
- Governing body ultimately responsible
  - Inherent in oversight function

How much is enough?

- Five components of a comprehensive framework of internal control
  1. Control environment
  2. Control activities
  3. Information and communication
  4. Monitoring activities
  5. Risk assessment

Recent modifications to the comprehensive framework

Internal Control — Integrated Framework (2013)

Background

- Why needed
  - Changing expectations
    - Governance
    - Fraud prevention and detection
  - Rapidly changing technology
  - Increasing complexity

What stays the same?

- Definition of *internal control*
- Five framework components

What changes?

- Principles-based approach to evaluating the effectiveness of internal control
  - Principles
    - Fundamental concepts associated with each component of internal control
  - Points of focus
    - Important characteristics of principles
- Guidance on evaluating effectiveness
  - Components and principles must be present and functioning
  - Components must be operating together

Entity Objectives

Part 2

Background

- All entities have a purpose
- Entity's goal = to achieve that purpose
- Performance subject to constraints

Three basic objectives

1. Operations objectives
   - Effectiveness
   - Efficiency
   - Safeguarding of assets against loss
2. Reporting objectives
   - Financial + nonfinancial
   - External + internal
3. Compliance objectives

1. Operations: effectiveness

- Meaning
  - Is the entity achieving its purpose?
- Risk
  - Presuming that past practice is effective without reference to mission, goals, and objectives

1. Operations: efficiency

- Meaning
  - Is the government making the best use of scarce resources?
- Risk
  - Focusing upon efficiency without first determining effectiveness
    - Something that is not effective cannot be efficient

1. Operations: safeguarding of assets against loss

- Meaning
  - Has the government taken appropriate steps to prevent the unauthorized acquisition, use, or disposition of assets
    - *Not* intended to encompass loss through waste, inefficiency, or poor business decisions
- Risk
  - Theft or misappropriation

2. Reporting

- Meaning
  - Does management have a reasonable basis for making assertions?
- Risk
  - Assuming responsibility *without having a reasonable basis* for doing so

3. Compliance

- Meaning
  - Ensure compliance (*before* the fact)
  - Demonstrate compliance (*after* the fact)
- Risk
  - Being satisfied with demonstrating compliance after the fact

Comprehensive Framework: Overview

Part 3

Component 1: Control environment

- Controls do not function in a vacuum
  - Is the environment favorable to internal control?
- Profoundly affects other components of internal control

Component 2: Risk assessment

- Ongoing process
  - Current risk exposure
  - Future changes

Component 3: Control activities

- Policies and procedures to address identified risks
  - Detection
  - Prevention

Component 2: information and communication

- Providing, sharing, and obtaining necessary information
  - Internally and externally
  - Upward and downward within the organization
- Essential to effectiveness of other components

Component 3: Monitoring activities

- Were controls implemented?
- Do they remain effective?
- Management's response

Inherent limitations

- Judgment
- External events outside the organization's control
- Breakdowns
- Management override
- Collusion

Individual Framework Components

Part 4

1.Control environment

Five related principles

Definition of control environment

- Set of standards, processes, and structures that provide the basis for carrying out internal control

Responsibility for control environment

- Governing body and senior management
  - Establish tone at the top regarding the importance of internal control
    - Including expected standards of conduct
- Management
  - Reinforces expectations at various levels of the organization

Relative importance of control environment

- Pervasive impact on the overall system of internal control
  - Importance impossible to exaggerate
    - Good environment - controls likely to function well
    - Bad environment - controls unlikely to function properly

Principle 1

- **The organization demonstrates a commitment to integrity and ethical values**
- Points of focus (4)
  - A. Organization sets the tone at the top
    - Governing body and management at all levels demonstrate importance of integrity and ethical values through
      - Directives
      - Actions
      - Behavior

Principle 1 (cont.)

B. Organization establishes standards of conduct
   - Understood at all levels, as well as by providers of outsourced services and by partners

C. Organization evaluates adherence to standards of conduct

D. Organization addresses deviations in a timely manner

Practical observations

- Attitude: essential tool or "red tape"
  - "Easier to ask forgiveness than permission"
  - "The talk" on "how things really work around here"
- Evidence of attitude
  - Time + money
  - How management deals with violations
- Force of bad example

Principle 2

- **The governing body exercises oversight of the development and performance of internal control**
- Points of focus (4)
  A. Governing body establishes oversight responsibilities
  B. Governing body applies relevant expertise
  C. Governing body operates independently
  D. Governing body oversees management's design, implementation and conduct of internal control

Audit committee

- Practical tool to allow governing body to exercise oversight responsibility for all aspects of internal control and financial reporting
- Direct line of communication between the governing body and the independent auditors
- Necessary for any government, regardless of size or type
- Membership
  - Members of the governing body
  - Assisted by financial expert

Audit committee (cont.)

- Must establish policy for dealing with complaints
  - Specifically provide for the confidential, anonymous submission by employees
- Provision for private meetings
  - To meet with independent auditors apart from management
  - To deliberate privately on conclusions

Principle 3

- **Management establishes, with governing body oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives**
- Points of focus (3)
  A. Management considers all structures of the entity
    - Operating units
    - Legal entities
    - Geographic distribution
    - Outsourced service providers

Principle 3 (cont.)

B. Management establishes reporting lines
   - Management designs and evaluates lines of reporting
     - Execution
     - Flow of information

C. Management and governing body define, assign, and limit authorities and responsibilities
   - Delegate authority
   - Define responsibilities
   - Use processes and technology to assign responsibility and segregate duties as necessary

Internal audit

- Practical tool to allow management to meet its internal control responsibilities
  - Additional time and expertise
- Structure options
  - Separate function
  - Outsourced
  - Regular staff
- Lines of reporting
  - Report to top management
  - Report to audit committee

Principle 4

- **The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.**
- Points of focus (4)
  A. Organization establishes policies and practices that reflect expectations of competence
  B. Governing body and management evaluate competence and address shortcomings

Principle 4 (cont.)

C. Organization attracts, develops, and retains individuals

- The organization provides the mentoring and training needed to attract, develop, and retain sufficient and competent personnel and outsourced service providers

D. Senior management and governing body plan and prepare for succession

- Contingency plans for assignment of responsibility

Practical observations

- Need for
  - Up-to-date job descriptions
  - Due diligence in hiring
    - Verifying credentials
    - Checking references
  - Ongoing training

Principle 5

- **The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives**
- Points of focus (5):
  A. Organization enforces accountability through structures, authorities, and responsibilities
     - Establishes mechanisms to communicate and hold individuals accountable for performance
     - Implements corrective action as necessary

Principle 5 (cont.)

B. Organization establishes performance measures, incentives, and rewards

C. Organization evaluates ongoing relevance of performance measures, incentives, and rewards

D. Organization considers excessive pressures

E. Evaluates performance and rewards or disciplines individuals

Practical observations

- Ensure that performance reviews are meaningful

2. Risk assessment

Four related principles

Risk

- Definition
  - Possibility that an event will occur and adversely affect the achievement of objectives
- Sources
  - External
  - Internal
- Assessment
  - Iterative process for identifying and assessing risks

Principle 6

- **The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives**
  - Organized consistent with three basic objectives
    - Operations objectives
    - Reporting objectives
    - Compliance objectives
  - 15 points of focus
    - Appropriate point of reference
    - Allowable variance
    - Representational faithfulness

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.**
- Points of focus (5)
  - A. Organization includes entity, subsidiary, division, operating unit, and functional levels
    - Identifies and assesses risks at each level
  - B. Organization analyzes internal and external factors

Principle 7 (cont.)

C. Organization involves appropriate levels of management

D. Organization estimates significance of risks identified

- Likelihood of risk occurring
- Potential impact
- Speed of impact
- Duration of impact

E. Organization determines how to respond to risks

- Accept, avoid, reduce, or share

Practical considerations

- Two goals
  - Assess current risk exposure
  - Anticipate future changes in risk exposure
    - Options decrease with the passage of time
    - Chances of success decrease with the passage of time

Practical considerations

- Inherent risk
  - Complexity
  - Cash receipts
  - Direct third-party beneficiaries
  - Prior Problems
  - Prior unresponsiveness to identified control weaknesses

Principle 8

- **The organization considers the potential for fraud in assessing risks to the achievement of objectives**
- Points of focus (4)
  A. Organization considers various types of fraud
  B. Organization assesses incentive and pressures
  C. Organization assesses opportunities
  D. Assesses attitudes and rationalizations

Principle 9

- **The organization identifies and assesses changes that could significantly impact the system of internal control.**
- Points of focus (3)
  - A. Organization assesses changes in the external environment
    - Regulatory, economic, and physical environment
  - B. Organization assesses changes in the business model
  - C. Organization assesses changes in leadership
    - Attitudes and philosophies

Practical observations

- Types of change
  - Operating environment
  - Personnel
  - Information systems and technology
  - Rapid growth
  - New programs and services

3. Control Activities

Three related principles

Definition of *control activities*

- Actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out

Principle 10

- **The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.**
- Points of focus (6)
  A. Organization integrates control activities with risk assessment
  B. Organization considers entity-specific factors

Principle 10 (cont.)

C. Organization determines relevant business processes
- Completeness
- Accuracy
- Validity

D. Organization evaluates a mixture of control activity types
- Authorizations and approvals
- Verifications
- Physical controls
- Controls over standing data
- Reconciliations
- Supervisory controls

Principal 10 (cont.)

E. Organization considers at what level activities are applied
F. Organization addresses segregation of duties

Practical considerations

- Authorization and approvals
  - Advance approval
    - Documentation of that fact
- Verifications
  - Comparisons – analytical review
    - Consistency with other financial data
    - Consistency with nonfinancial data
    - Consistency with expectations
- Physical controls
  - Assignment of responsibility for "walk-away" items

Practical considerations (cont.)

- Segregation of incompatible duties
  - Alternatives available when not cost effective

Principle 11

- **The organization selects and develops general control activities over technology to support the achievement of objectives.**
- Points of focus (4)
  A. Organization determines dependency between the use of technology in business processes and technology general controls
  B. Organization establishes relevant technology infrastructure control activities

Principle 11 (cont.)

C. Organization establishes relevant security management process control activities

D. Organization establishes relevant technology acquisition, development, and maintenance process control activities

Principle 12

- **The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.**
- Points of focus (6)
  - A. Organization establishes policies and procedures to support deployment of management's directives
    - Policies = what is expected
    - Procedures = specific actions
  - B. Organization establishes responsibility and accountability for executing policies and procedures

Principle 12 (cont.)

- Points of focus (cont.)
  - C. Organization performs in a timely manner
  - D. Organization takes corrective action
  - E. Organization performs using competent personnel
    - Sufficient authority
    - Diligence and continuing focus
  - F. Organization assesses policies and procedures
    - Continued relevance
    - Refresh as necessary

4. Information and communication

Three related principles

Information

- Needed
  - For internal control
  - To meet objectives
- Sources
  - Internal
  - External

Communication

- Providing, sharing, and obtaining information
- Continual and iterative process
- Internal
  - Up, down, and across
- External
  - Inbound
  - Outbound

Practical considerations

- Relationship to other components of the internal control framework
  - Does not exist separately from other components

Principle 13

- **The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.**
- Points of focus (5)
  A. Organization identifies information requirements
  B. Organization captures internal and external sources of data
  C. Organization processes relevant data into information

Principle 13 (cont.)

D. Organization maintains quality throughout processing
   - Timely
   - Current
   - Accurate
   - Complete
   - Accessible
   - Protected
   - Verifiable
   - Retained
   - Reviewed for relevance

E. Organization considers costs and benefits

Principle 14

- **The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.**
- Points of focus (4)
  - A. Organization communicates internal control information
    - Information needed to understand and carry out responsibilities
  - B. Organization communicates with the governing body

Principle 14 (cont.)

C. Organization provides separate communications lines
   - Fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective

D. Organization selects relevant method of communication
   - Considers
     - Timing
     - Audience
     - Nature of information

Practical considerations

- Direction of communication
  - From top management down through the organization
  - From lower levels up to top management
  - Laterally within the organization

Practical considerations (cont.)

- Documentation of policies and procedures
  - Promulgate in a manner that emphasizes importance
  - Update
    - On predetermined schedule
    - When changes occur
  - Employee assigned for the purpose
    - Management to oversee performance in this regard
  - Readily available
  - Clear delineation of authority and responsibility
  - Explanation of purpose and design

Principle 15

- **The organization communicates with external parties regarding matters affecting the functioning of internal control.**
- Points of focus (5)
  A. Organization communicates to external parties
  B. Organization enables inbound communications
  C. Management communicates with the governing body
  D. Organization provides separate communications lines
  E. Organization selects relevant method of communication

5. Monitoring

Two principles

Types of evaluations

- Ongoing evaluations
  - Built into business processes
- Separate periodic evaluations
  - Scope and frequency dependent upon
    - Assessment of risks
    - Effectiveness of ongoing evaluations
    - Other management considerations
- Combination

Goal of evaluations

- Ascertain whether
  - Each of the five components
    - Present and functioning
  - Each of the principles within each component
    - Present and functioning

Findings of evaluations

- Evaluate against criteria
  - Regulators
  - Standard-setting bodies
  - Management
  - Governing body
- Communicate deficiencies
  - Management
  - Board of directors

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.**
- Point of focus (7)
  A. Organization considers a mix of ongoing and separate evaluations
  B. Organization considers rate of change
  C. Organization establishes baseline understanding

Principle 16 (cont.)

D. Organization uses knowledgeable personnel

E. Organization integrates with business processes

- Builds in
- Adjusts to changing conditions

F. Organization adjusts scope and frequency

- Dependent on risk

G. Organization objectively evaluates

- Separate evaluations performed periodically to provide objective feedback

Practical considerations

- Establishing a baseline
  - Essential elements
    - Identification of risk
    - Determination of risk appetite
  - Determine that compensating controls are present and consistent with risk appetite
  - Determine whether the design of compensating controls is adequate
  - Determine whether compensating controls have been fully implemented

Practical considerations (cont.)

- Updating the baseline
  - To reflect changes in
    - The processes that are the object of controls
    - The controls themselves
      - Elimination of use of lockbox for collections
    - Risk exposure
  - Process for updating
    - Periodic reviews
    - When changes occur

Practical considerations (cont.)

- How have identified deficiencies been resolved?
  - Human response is an integral part of the effectiveness of the control

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.**
- Points of focus (3)
  A. Management and governing body assess results

Principles 17 (cont.)

B. Organization communicates deficiencies
   - Parties responsible for taking corrective action
   - Senior management
   - Board of directors

C. Organization monitors corrective action
   - Management tracks timely remediation

Practical considerations

- Resolving deficiencies
  - Focus on root cause of deficiencies
  - Corrective action plan
    - Timetable
    - Follow-up plan
  - Reporting
    - Responsible individual
    - Individual at least one level above responsible individual

Summary

- COSO 2013
  - Expands COSO 1992
    - Associates *principles* and *points of focus* with individual framework components
    - Provides guidance on how to evaluate results of an assessment
      - All components and principles must be present
      - Components must work together
    - Treats safeguarding of assets as a separate element within operations objectives
- New GFOA Elected Officials Guide available
- New full-length publication scheduled for 2016