# Updates to the Standards for Internal Control in New York State Government

Presented to the New York State Internal Control Association

John Buyce
Amanda Strait
May 1, 2014

# Reasons for Update

- The Standards were last revised in 2007

- In May 2013, the Committee of Sponsoring Organization of the Treadway Commission (COSO) updated its Internal Control–Integrated Framework.

# COSO Update

- Builds on what was useful in the past
- Retains the core definition of internal control and the five components on internal control
- Provides clarity to the user in designing and implementing systems of internal control

# COSO Update

- Formalizes fundamental concepts as 17 principles associated with the five components
- Increases relevance and dependence on Information Technology
- Includes the performance of a Fraud Risk assessment

# Control Environment

- Integrity and Ethics
- Oversight responsibility
- Responsibility/Authority
- Competence
- Enforces Accountability

# Risk Assessment

- Objectives
  - Operations
  - Reporting
  - Compliance
- Analyzes Risk
- Analyzes Fraud
- Analyzes Change

# Control Activities

- Develops Controls
- Technology Controls
- Policies and Procedures

# Information and Communication

- Relevant Information
- Communicates Internally
- Communicates Externally

# Monitoring Activities

- Conducts ongoing/separate evaluations
- Evaluates and communicates deficiencies

# Key Changes to Standards

- Four Purposes verses Three Objectives
- Why are Internal Control Important
- Fraud Risk
- Information Technology Risk
- Managing the Internal Control System

# Part 1: Internal Control Framework

- 2007 Definition
  - Internal control is the integration of the activities, plans, attitudes, policies, and efforts of the people of an organization working together to provide reasonable assurance that the organization will achieve its objectives and mission.

- New 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 relating to operations, reporting, and compliance.

Mission Focus

Focus on Management Responsibility

# Fundamental Concepts and Expectations

- Affects every aspect of an organization: all of its people, processes and infrastructure;
- Is a basic element that permeates an organization, not a feature that is added on;
- Incorporates the qualities of good management;
- Is dependent upon people and will succeed or fail depending on the attention people give to it;
- Is effective when all of the people and the surrounding environment work together;
- Provides a level of comfort regarding the likelihood of achieving organizational objectives; and
- Helps an organization achieve its mission.

## 2007 Version

- Geared to the achievement of objectives in one or more of the following categories—operations, reporting, and compliance;
- A process consisting of ongoing tasks and activities;
- Effected by people—it is about people and the action they take at every level in a organization, not just about the policy and procedure manuals, systems, and forms. Internal control will succeed or fail depending on the attention people give it;
- Able to provide reasonable—but not absolute—assurance to an entity's senior management and board of directors;
- Adaptable to the entity structure—flexible in application for the entire entity or for a particular subsidiary, division, operating unit, or business process

## 2014 Draft

# 2007 – Four Purposes of Internal Control

- Promote orderly, economical, efficient and effective operations, and produce quality products and services consistent with the organization's mission.
- Safeguard resources against loss due to waste, abuse, mismanagement, errors and fraud.
- Promote adherence to laws, regulations, contracts and management directives.
- Develop and maintain reliable financial and management data, and accurately present that data in timely reports

Operations & Assets

Compliance & Reporting

# 2014 – Three Objectives of Internal Control

- **Operations Objectives:**
  - Pertaining to effectiveness and efficiency of the entity's operations, including operational and financial performance goals. These objectives promote orderly, economical operations and help produce quality products and services consistent with the organization's mission. They also serve to safeguard resources against loss due to waste, abuse, mismanagement, errors and fraud.

- **Reporting Objectives:**
  - Relating to internal and external financial and non-financial reporting. These objectives may encompass reliability, timeliness, transparency, or other terms as set forth by regulators, recognized standard setters, or the entity's policies.
- **Compliance Objectives:**
  - Dealing with adherence to laws, regulations, contracts and management directives to which the entity is subject.

1st & 2nd Purposes

3rd & 4th Purposes

# New Item: Why Internal Controls are Important

- Help organizations accomplish their missions;
- Reduce opportunities for fraud;
- Prevent loss of funds or other resources;
- Establish standards of performance;
- Ensure compliance with laws, regulations, policies and procedures;
- Preserve integrity;
- Discourage bad publicity;
- Ensure public confidence, and
- Protect all employees.

Critical Benefits

# Organizational Roles

- Everyone has a role
- Greatest responsibility lies with Management
  - Especially the “Top Executive”
- Internal Control Officer

2007

- Largely unchanged
- “Executive Operational Head” of the organization

2014

# Internal Control Components

- Control Environment
- Communication
- Assessing & Managing Risk
- Control Activities
- Monitoring

2007

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

2014

# Control Environment

- Governance
- Ethical Values & Integrity
- Management Operating Style & Philosophy
- Competence
- Morale
- Supportive Attitude
- Mission
- Structure

2007

- Some small additions
  - "Attitude" toward internal control
  - Openness & responsiveness
  - Holding individuals accountable
  - Fair, consistent, timely discipline
  - Succession & contingency planning

2014

# Information & Communication

- Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of other components of internal control.

- The continual, iterative process of providing, sharing, and obtaining necessary information.
- It enables personnel to receive a clear message from senior management that control responsibilities must be taken seriously.

Information

Communication

# Information & Communication

- All aspects of a strong internal control system are reliant on timely, relevant and accurate communication methods.
- An organization must internally communicate information, including objectives and responsibilities for internal control, to support the functioning of all other components of the internal control system.

# Risk Assessment

- Preparing to Assess Risk
- Risk Assessment Process
- Managing Risk
- Preventing or Reducing Risk
- Managing Risk During Change

- Two new items added
- Fraud Risk
- Information Technology Risk

2007

2014

# Preparing to Assess Risk – Subtle Changes

- Risk should be assessed and managed through an organization-wide effort to identify, evaluate and monitor those events that threaten the accomplishment of the organization's mission.

2007

- Risk is the possibility that an event will occur and threaten or otherwise adversely affect the achievement of objectives
- Risk management is an ongoing process that must include monitoring the changing environment and tracking planned actions to mitigate the impact and likelihood of risks.

2014

# More Purposes vs. Objectives

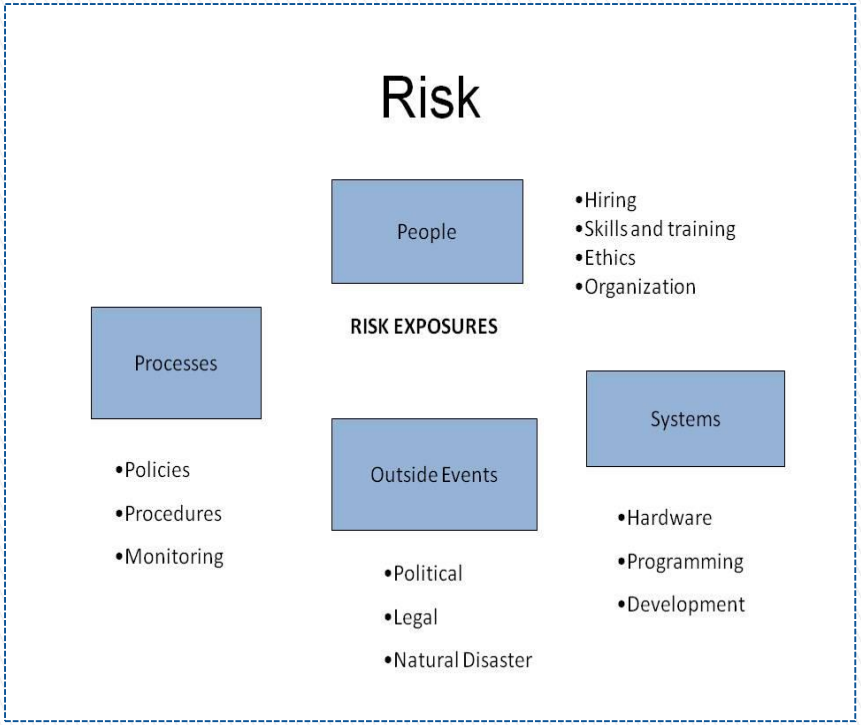
- Management should first ensure that it has identified all the operational and control objectives throughout the organization.
- Control objectives are generally derived from the four purposes of internal control

2007

- Management first needs to identify all business objectives of its programs and units, including operational goals, reporting, and compliance requirements
- Business objectives should flow from the three objectives of internal control

2014

# New Discussion of Risk




- People
- Processes
- Systems
- Outside Events

Risk Exposures

Factors Impacting Risk

# Fraud Risks

- Fraud is any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain.

- All organizations need to consider the potential for fraud to occur
- Can be documented separately or in conjunction with other risks

Fraud Defined

New Requirements

# Factors to Consider & Assess

- **Types of Fraud**
  - e.g., fraudulent reporting, possible loss of assets, and corruption
- **Incentives and Pressures**
  - internal and external motives and demands.
- **Opportunities**
  - unauthorized acquisition, use, or disposal of assets
  - altering of the entity's reporting records, or
  - committing other inappropriate acts
- **Attitudes and Rationalizations**
  - how management and other personnel might justify inappropriate actions

# Information Technology Risk

- Growth and technology advances expose organizations to greater risks
- Organizations must identify and assess the risks accompanying each new device, platform, software application or business model

- How does the new technology contribute to achieving the organization's mission?
- Does the new technology increase risks that may hinder the accomplishment of objectives? (e.g., reduced data security, frequent or prolonged service interruptions, steep learning curves, or decreased morale)
- What changes to control activities are necessary to manage these risks?

Technology Risks

Questions to Ask

# Managing Risk

## Three Options

- *Accept the risk:* Do not establish control activities
- *Prevent or reduce the risk:* Establish control activities
- *Avoid the risk:* Do not carry out the function

## 4th Option

- *Transfer or share the risk*
  - Management may transfer responsibility for all or part of the risk to a service provider or business partner
    - (IT Systems)

2007

2014

# Managing Risk

- In most cases, government entities do not have the ability to eliminate programs to wholly avoid risks
- Options to share or transfer risks to others are also limited.

- As a result, management must most often take actions to reduce risks to acceptable levels.

Limitations

Approach

# Control Activities – Little change

- Tools that help identify, prevent or reduce risk

- Actions established through policies that establish what is expected and procedures that put those policies in action.

| 2007 | 2014 |
| --- | --- |

# Control Activities for IT

- Mini-computers
- Dial-up numbers
- Dial-back access
- Office for Technology

- Server networks
- Virtual private networks
- Office of Information Technology Services

Old references deleted

New references added

# Monitoring – Minor additions

- Independent evaluations should be performed periodically to provide objective feedback.

- Management must evaluate and communicate 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.

# New Part III – Managing & Evaluating the Internal Control System

- Incorporates & elevates the importance of the prior Supporting Activity of called “Evaluation”

- Key components:
  - Responsibility for Managing the System
  - Importance of Internal Control & Risk Management
  - Managing the System
  - Evaluation

# Key Points

- The internal control or risk management function is responsible for identifying and inventorying risks to the mission of the organization on both a unit- and entity-wide basis
- The operation and monitoring of the system of internal control should be undertaken by individuals who collectively possess the necessary skills, technical knowledge, objectivity, and understanding of the organization

# Responsibility

- External and internal auditors are not responsible for an entity's internal controls.
  - External auditors evaluate internal controls as part of their audit planning process to determine if they can be relied on
  - Internal auditors assess whether an organization's internal controls are effective and evaluate the way an organization operates
  - Neither is responsible for the design and effectiveness of controls

# Who is responsible?

- An organization's management (including any applicable governing board) is responsible for making sure that the right controls are in place, and that they are performing as intended.

# Internal Control Responsibilities

- Oversight of the system
- Authorization for policies and initiatives
- Ethical leadership

Board, Commissioner, etc.

- Create the policies needed to ensure that the organization accomplishes its mission
- Work with managers and department heads to recommend and implement procedures that lower identified risks

Executive Operational Head (Exec. Dep., Dep. Director, etc.)

# Key Issues in Managing the System

- Identifying the organization's risk tolerance (e.g., margin of error, materiality) and what is deemed an unacceptable event
- Conducting ongoing environmental scans of legislation, market condition or political changes and resulting potential impact on the organization
- Performing internal assessments of entity-wide risk, both actual and potential, with mitigation strategies

# Other Key Aspects

- The system of control should be embedded in the operations of the company and form part of its culture.
- Controls should be capable of responding quickly to evolving risks, both internal and external.
- The costs of control must be balanced against the benefits, including the risks it is designed to manage.

# Other Key Aspects

- The system of control must include procedures for reporting immediately to appropriate levels of management any significant control failings, or weaknesses that are identified, together with details of corrective action being undertaken

- Control can help minimize the occurrence of errors and breakdowns but cannot provide absolute assurance that they will not occur

# Part IV – Supporting Activities

- Evaluation
  - No longer a distinct activity
  - Incorporated into new “Managing” section
- Strategic Planning
  - Largely unchanged
- Internal Audit
  - Largely unchanged
  - Emphasis on preserving independence

# Appendix – Internal Control References

- Updated References

- Additional References
  - NYS Guide to Financial Operations – Contract Monitoring
  - NYS Guide to Financial Operations – Certification of Internal Control Over the Payment Process
  - Requests to get specialized training on Internal Controls – Outreach@osc.state.ny.us

# What have we missed?

- Are there other key aspects of the COSO revision that you think need to be addressed or incorporated?
- Are there other issues outside of COSO that need to be addressed?

# Contact Info

John Buyce
Audit Director

jbuyce@osc.state.ny.us

(518) 473-8757

Amanda Strait
Associate Examiner

Astrait@osc.state.ny.us

(518) 474-3271