

# Standards for Internal Control in New York State Government 2016 Update

Presented to the New York State Internal Control Association

John F. Buyce

Audit Director

April 28, 2016



NYS COMPTROLLER  
**THOMAS P. DiNAPOLI**

---

# Last Revised in 2007

A lot has happened since then....

- **Recession & White Collar Crime**
  - Focus on Fraud Prevention & Detection
  - Emphasis on Risk Management
- **Prosecution of Public Officials**
  - Accountability & Transparency
- **Technological Advances**



# Also in the Last Decade

The really important stuff.....

- **Series of Internal Control Audits**
  - 2008 – Were the annual Certs following B-350?
  - 2012 – Were they timely, complete, documented?
  - 2014 – Are we addressing all the components?
- May 2013, COSO updated its Internal Control-Integrated Framework.
- September 2014 – GAO updated its Green Book



# Key Objectives

- ▶ Build on what has been useful.
  - Keep the core concepts
  - Provide greater clarity in important areas
  - Stay up to date and even expand our approach
- ▶ Continue taking us to the next level
  - More fully integrated, but flexible, internal control systems
  - Greater focus on managing the systems instead of just establishing and maintaining them



# Effective Dates

- The updated Standards are effective now. Although COSO's updated Internal Control Framework has been around since 2013, some agencies may need to complete a transition.
- Agencies should ensure full Implementation during fiscal year 2016/17, with expectation of complete integration into their operations by March 31, 2017



# Core Expectations

- Each agency must have a process to assure itself that controls are both adequate and functioning as intended.
- It needs to be a continuous process.
- Everyone is responsible for internal control, but they have different roles.



# Core Expectations - ICOs

- ICO needs to have a broad understanding of agency operations
- ICO must report to agency head – Direct line of communication to executive management
- ICO needs to have sufficient authority to act for the agency head on issues related to IC
- Cannot be the Internal Auditor
- Internal Control Officers are not responsible for the system; their role is to help facilitate, document and assess all of the components.



# Key Changes to the Standards

- Incorporates COSO's 2013 updated Internal Control Framework, but adapts it to better fit the government structure.
  - Emphasizes the need to Actively Manage the Internal Control System
  - Recognizes increased relevance and dependence on Information Technology
  - Requires specific consideration of Fraud Risks
  - Emphasizes the importance of system documentation



# 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.

Mission Focus

## ▶ 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.

Focus on Management Responsibility

# Fundamental Concepts and Expectations

- ▶ Helps an organization achieve its mission.
- ▶ Provides a level of comfort regarding the likelihood of achieving organizational objectives;
- ▶ Geared to the achievement of objectives in one or more of the following categories—operations, reporting, and compliance;
- ▶ Able to provide reasonable—but not absolute—assurance to an entity’s senior management and board of directors;

2007 Version

2016 Update

# 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;
- ▶ Adaptable to the entity structure—flexible in application for the entire entity or for a particular subsidiary, division, operating unit, or business process
- ▶ A process consisting of ongoing tasks and activities;

2007 Version

2016 Update

# Fundamental Concepts and Expectations

- ▶ 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;
- ▶ 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;

2007 Version

2016 Update

# 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.
- ▶ Develop and maintain reliable financial and management data, and accurately present that data in timely reports
- ▶ Promote adherence to laws, regulations, contracts and management directives.

Operations & Assets

Reporting & Compliance

# 2016 – 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.

1<sup>st</sup> & 2<sup>nd</sup> Purposes

## ▶ 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.

3<sup>rd</sup> & 4<sup>th</sup> Purposes

## New Item: Importance of Internal Control and Risk Management

- ▶ Help organizations accomplish their mission and objectives;
- ▶ 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
- ▶ Largely unchanged
- ▶ More discussion about the role of the “Executive Operational Head” of the organization

2007

2016

# Minimum Documentation Requirements

Some flexibility based on agency complexity, but some items are mandatory

- Decision that a Principal is not relevant, and describe compensating controls
- Policies should document relevant Internal control responsibilities
- Evaluation of operations, risks and identified vulnerabilities
- Results on ongoing monitoring & evaluations
- Internal control issues and timely corrective actions



# Internal Control Components

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

2007

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

2016

# Control Environment

- ▶ Governance
  - ▶ Ethical Values & Integrity
  - ▶ Management Operating Style & Philosophy
  - ▶ Competence
  - ▶ Morale
  - ▶ Supportive Attitude
  - ▶ Mission
  - ▶ Structure
- ▶ Some small additions
    - “Attitude” toward internal control
    - Open & responsive
    - Holding individuals accountable
    - Fair, consistent, timely discipline
    - Succession & contingency planning

2007

2016

# Control Environment

## First 5 Core Principles:

- ❖ Demonstrates Commitment to Integrity and Ethical Values
- ❖ Exercises Oversight Responsibility
- ❖ Establishes Structure, Authority and Responsibility
- ❖ Demonstrates Commitment to Competence
- ❖ Enforces Accountability



# Demonstrates Commitment to Integrity & Ethical Values

## Integrity

- Encourages honesty & fairness
- Respects the organization
- Respects employee rights
- Respects authority
- Leads by example
- Committed to excellence
- Complies with laws & policies
- Adheres to professional standards

## Ethical Values

- Establishes a code of conduct and complies with it
- Rewards employee commitment to ethical values
- Provides method to report ethical violations
- Consistently enforces disciplinary practice



# Demonstrates Commitment to Competence

- Establishes knowledge & skill requirements for all positions
- Verifies qualifications of all candidates
- Hires and promotes only those who have the required knowledge and skills
- Establishes training and education programs to help employees improve knowledge and skills
- Plans and prepares for succession through contingency planning



# 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

2016

# Risk Assessment

- ▶ Four Core Principles:
    - ❖ Specifies suitable objectives
    - ❖ Identifies and analyzes risk
    - ❖ Assesses fraud risk
    - ❖ Manages risk during change
- 

## 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.
- ▶ 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.

2007

2016

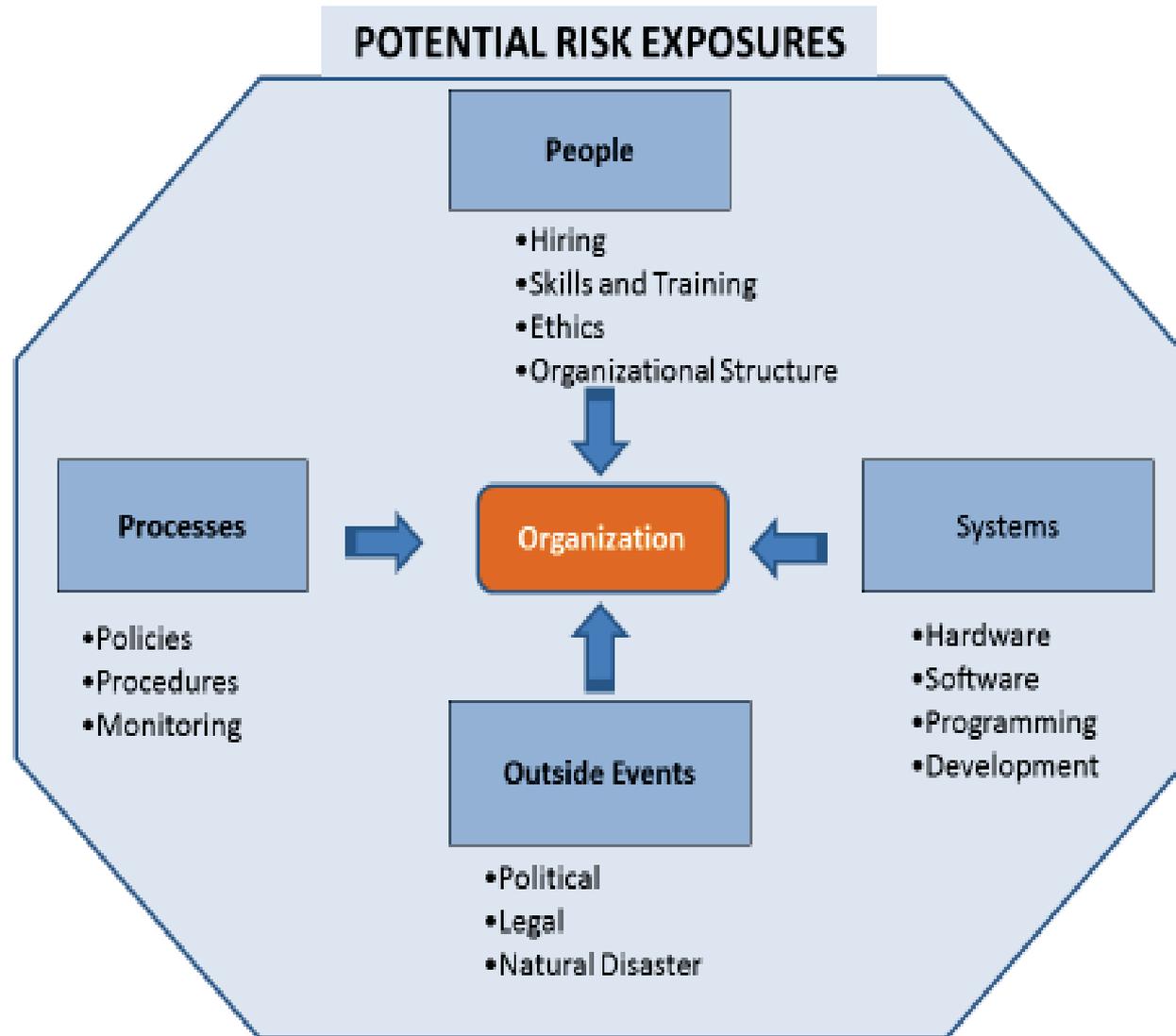
# More Purposes vs. Objectives

- ▶ 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
- ▶ 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

2007

2016

# New Discussion of Risk



# 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

# Consideration of 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

# 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

2016

# 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

## Three Core Principles:

- ❖ Selects and develops control activities
- ❖ Selects and develops general controls over technology
- ❖ Deploys controls through policies and procedures



# 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

2016

# 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

# Information and Communication

- ▶ Three Core Principles:
    - ❖ Uses relevant information
    - ❖ Communicates internally
    - ❖ Communicates externally
- 

# 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 communicate information, including objectives and responsibilities for internal control, to support the functioning of all other components of the internal control system.

Both Internally

and Externally

# Monitoring

- ▶ Final Two Core Principles:
  - ❖ Conducts ongoing and/or separate evaluations
  - ❖ Evaluates and communicates deficiencies

## 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

## 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

- ▶ Auditors (external or internal) 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
- ▶ Create the policies needed to ensure that the organization accomplishes its mission & objectives
- ▶ Work with managers and department heads to recommend and implement procedures that lower identified risks

Board, Commissioner, etc.

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 agency and form part of its culture.
  - ▶ Controls should be flexible and 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](mailto:Outreach@osc.state.ny.us)

# Take Aways

- ✓ No real change in the fundamentals; just more detail to help you assess the adequacy of the system
- ✓ Need to clearly document each of the elements and how your organization has addressed them



# Take Aways

- ✓ Internal controls can not be stand alone efforts; all the principles need to be imbedded in the organization's way of operating.
- ✓ The internal control system needs to be continuously managed – it should not be a one time event – but rather ongoing and forward-looking



# Take Aways

- ✓ The new Standards are in effect now, but won't start looking for full compliance in audits until the transition year is complete.

