Internal Control Monitoring Plan Guidance

October 22, 2015

Table of Contents

Part I: Introduction

The four basic functions of management are usually described as planning, organizing, leading, and controlling. Internal control is what is meant when discussing the fourth function, controlling. Adequate internal controls allow managers to delegate responsibilities to staff with reasonable assurance that what they expect to happen, actually does. Internal control is an integral part of managing an organization. It comprises the plans, methods, and procedures used to meet missions, goals, and objectives and, in doing so, supports performance-based management systems. Internal control also serves as the first line of defense in safeguarding assets and preventing and detecting errors and fraud. In short, internal control, which is synonymous with management control, helps government managers achieve desired results through effective stewardship of public resources.

Purpose of Guide

In accordance with *Management Directive 325.12, Standards for Internal Controls in Commonwealth Agencies*, agencies under the Governor's jurisdiction must adopt and implement the internal control framework outlined in *Standards for Internal Control in the Federal Government* (Green Book). As noted in this directive, the standards must be applied to all aspects of an agency's operations, reporting, and compliance with applicable laws and regulations, regardless of the funding source. Agencies must use the components, principles, and attributes of the Green Book to design, implement, operate, and assess an effective internal control system. This directive also requires agencies to document the results of ongoing internal and external monitoring and evaluation of their agency's internal control system. This document provides agencies with guidance as to the development of a comprehensive internal and external monitoring plan to ensure sufficient controls exist, provide for the required accountability and transparency, and ensure that the relevant internal control objectives are met. This guidance will address both the agency's need to monitor its own internal controls and the need to monitor its subrecipients, if applicable. If there are questions, please forward them to the Management Directive 325.12 resource account.

Since internal control is a dynamic process that has to be adapted continuously to the risks and changes an entity faces, monitoring of the internal control system is essential in ensuring that the internal controls remain aligned with changing objectives, environment, laws, resources, and risks. Internal control monitoring assesses the quality of performance over time and can resolve the findings of audits and other reviews. Corrective actions are a necessary complement to control activities in order to achieve objectives. Consequently, it is essential that a dynamic internal control monitoring plan be developed to achieve these objectives. This guide serves as a conduit for accomplishing this purpose.

What Are Internal Controls?

In the **Green Book**, the US Government Accountability Office (GAO) defines internal control as a process affected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved. These objectives and related risks can be broadly classified into one or more of the following three categories:

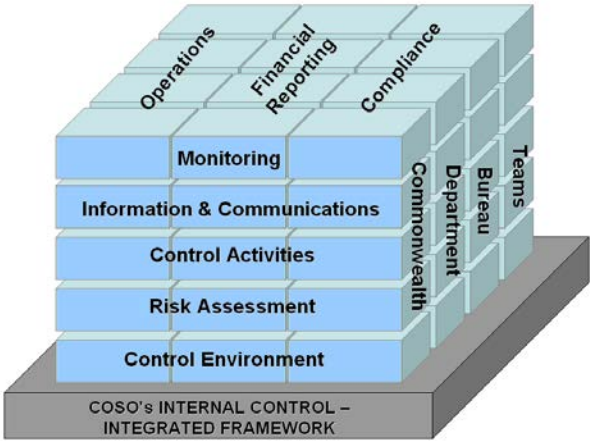
* Operations - Effectiveness and efficiency of operations

* Reporting - Reliability of reporting for internal and external use

* Compliance - Compliance with applicable laws and regulations

Management uses internal control to help the organization achieve these objectives. While there are different ways to present internal control, the Green Book approaches internal control through a hierarchical structure of 5 components and 17 principles. The 5 components of internal control are Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring. These 5 components represent the highest level of the hierarchy of standards for internal control and must be effectively designed, implemented, and operating in an integrated manner for an internal control system to be effective.

The cube below represents the integrated framework developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) for assessing and improving internal control systems. The Green Book adapts these principles for a government environment. The internal control system is a dynamic and integrated process in which each of the five components impact the effectiveness of the other components. A relationship exists not only between the components, but also the objectives and the agency's organizational structure.



The three categories into which an agency's objectives can be classified are represented by the columns labeled on top of the cube. The 5 components of internal control are represented by the rows. The organizational structure is represented by the third dimension of the cube.

This definition denotes certain fundamental concepts that internal controls:

- affect every aspect of an agency: all of its employees, processes and infrastructure.
- are not stand-alone practices. They are woven into the day-to-day responsibilities of managers and their staff.
- incorporate the qualities of good management.

- are dependent upon people and will succeed or fail depending on the attention people give to it.

- must make sense within each agency's unique operating environment and are effective when people work together.

- provide a level of assurance to an agency, but does not guarantee success.

- help an agency achieve its mission.

- should be cost effective.

Preparing the Plan

In accordance with *Management Directive 325.12, Standards for Internal Controls in Commonwealth Agencies*, agency heads are required to provide an annual monitoring plan for their agency. To this end, appropriate management staff should be assigned to assist in developing and providing updates to the monitoring plan. The plan will describe how the agency expects to meet its unique goals and objectives by using policies and procedures to minimize risk.

In preparing the monitoring plan, agencies can utilize the Internal Control Assessment Template in order to perform an initial assessment of the internal control system. The results of this assessment along with addressing the 5 components and 17 principles in Five Standards of Internal Control (Part II) of this guide would serve as a blueprint for the plan. The use of these components rather than a "canned" or strict step-by-step method will provide agencies with a certain level of flexibility in developing their internal control plan. Evaluating, identifying and documenting current internal controls is the first step toward preparing a monitoring plan. The monitoring plans can take many different forms, depending on the organizational structure and business practices of the agency. In general, however, the monitoring plan should:

•Discuss the goals and objectives of your agency;
•Briefly state the integrity and ethical values expected of all staff, and especially the ethical values top management expects of itself (control environment);
•Describe the risks to meeting goals and objectives;
•Explain how the structure, policies, and procedures of the agency act to control the risk (control activities); and,
Specify the methods for monitoring the controls

How voluminous or detailed the plan is or what documentation is contained in the plan depends on a number of factors, including an agency's size, the complexity of its organizational structure, and the functions it performs. The plan may contain copies of or links to policy and procedures manuals, flowcharts of processes, agency mission statements, an affirmation signed by the agency head supporting the agency's efforts to improve its internal control structure, and a description of how the agency intends to monitor its internal control system. The plan's contents will vary by agency. However, the information required to document a specific agency's plan should become apparent as the agency works through Part II.

Assessable Unit Determination

To perform an orderly, systematic evaluation of the system of internal control, management should segment the agency into "assessable units." An assessable unit has certain primary characteristics. It has an ongoing, identifiable purpose that results in the creation of a service or product (used either internally or externally) and/or that fulfills a law, regulation or other mandate. An assessable unit should be large enough to allow managers to evaluate a significant portion of the activity being examined, but not so large that managers cannot perform a meaningful evaluation without extensive time and effort.

An agency can be segmented according to the following two basic approaches:

1. Transaction cycle approach

2. Organizational structure approach.

For the first approach, *transaction cycle approach*, appropriate functional transactional cycles must be identified. A transaction cycle is a stream of related events and processes which satisfy one overall functional need of the agency.

This method will result in broad assessable units (cycles) such as the revenue cycle, disbursement cycle, and budget cycle which cut across organizational lines. For example, the budget transaction cycle would include processes performed in the agency's budget office (if applicable) as well as in the agency's administrative and fiscal offices.

This method best clarifies the interaction of controls between different segments. Controls in each segment will be evaluated and reviewed to see how they affect the agency as a whole. The transaction cycle approach might be preferred for a small agency which is not as organizationally complex as a large agency.

The drawbacks of this method include the need to cross over organizational lines of authority, often involving many managers, and the lack of organizational structure along cycle lines. These drawbacks can impede an orderly and successful evaluation.

The *organizational structure approach* involves delegating internal control responsibilities to managers along formal organization lines. Factors to be considered in segmenting the agency into assessable units under this method are as follows:

- Organization Chart - Segmentation that closely follows the agency's formal structure is usually efficient and effective when the organizational lines are clearly shown. When lines of authority and reporting responsibilities are interwoven, the organization chart becomes less useful as a tool for segmentation.

- Physical Location – An agency's programs or administrative functions could operate in several locations. Since the control systems may vary among locations, it may be necessary to perform separate evaluations at each location. On the other hand, if an agency's operations are confined to one location, it may be appropriate to have assessable units that include more functions.

- Autonomy - The more independent a function, the more likely the function should be considered a separate assessable unit.

- Materiality - An important consideration in any agency is the commitment of personnel and dollars. The larger the program area, the greater the likelihood that the function should be considered a separate assessable unit.

When segmenting the agency, any associated support activities (cash receipts, cash disbursements, etc.) must be examined to determine whether they should be a separate assessable unit based on the degree of centralization and control. The greater the autonomy, the greater the risk and, therefore; the greater the need for accountability and emphasis of this function as a separate assessable unit. For example, some support activities may be centralized at the Secretary organizational level. These activities should be studied to determine the extent of its control and responsibility to decide if it should be segregated as separate assessable units.

Examples of support activities that could be considered assessable units at the agency level are:

- Strategic and Long-Range Planning - This involves establishing and implementing broad, long-range goals and objectives. This process is important since it charts the general direction of the entity for the future.

- Operational Planning - This concerns setting objectives for the current budget cycle. The annual budget expresses the current year's objectives in financial terms.

- Program Operations, Planning, and Management - This includes maintaining performance standards and reports so that management may analyze performance (such as construction completion milestones, claims administered per employee, accounts processed for collection and transactions processing time).

- Cash Receipts/Revenue/Sales - This activity includes all actions associated with the receipt, depositing and safeguarding of cash, including imprest/working funds.

- Cash Disbursements/Procurement - This concerns all of the purchasing processes, accounting for the related liabilities and authorizations for payment.

- Human Resources - This activity encompasses all duties and procedures related to time, attendance and payroll functions performed within the organization.

- Property, Plant, and Equipment - This includes all policies, procedures and operations concerning the acquisition, maintenance and disposition of the agency's fixed assets, including accounting.

- Information Technology Systems - This includes general and application controls on electronic data processing.

The advantages of segmenting on an organizational basis include:

- An agency manager is usually in place that has authority and responsibility for internal controls.

- There is a greater understanding of operations by personnel.

- It is easier to segment an agency along lines of authority and responsibility that already exist.

A disadvantage of this method is that the flow of transactions may be disrupted. For example, information regularly flows between personnel, payroll, and accounting activities. Breaking these activities along organizational lines may cause inefficiencies later in the evaluation process.

All important functions and activities must be included in the assessable unit. The exclusion of activities from an agency may result in improper management conclusions on the activities subject to the risk assessment and on the agency's overall internal control structure.

The agency's assessment of internal control can be performed using a variety of information sources. Management has primary responsibility for assessing and monitoring controls on an ongoing basis, and should use other sources as a supplement to, not a replacement for, its own judgment. Sources of information include:

- Management knowledge gained from the daily operation of programs and systems

- Management reviews conducted: (i) expressly for the purpose of assessing internal control, or (ii) for other purposes with an assessment of internal control as a byproduct of the review

- Reports, including federal agencies' audits, legislatively mandated audits, Single Audit report findings for agencies receiving federal funding, inspections, reviews, investigations and outcomes of hotline complaints or other products

- Program evaluations

- Audits of financial statements, including information revealed in preparing the financial statements; the auditor's reports on the financial statements, internal control, and compliance with laws and regulations; and any other materials prepared relating to the statements

- Control Self Assessments

- Other reviews or reports relating to agency operations

Identifying manageable assessable units of an agency's activities ensures that:

1. All important inherent risks are identified
2. Meaningful evaluations are made to determine if the environment is conducive to effective internal control techniques

3. Knowledgeable individuals assess the design and operation of internal controls in meeting their stated objectives.

After each assessable unit has been identified, the Oversight Body should name a project lead **and maintain a listing of the agency's assessable units.**

The project leads of the assessable units should have the responsibility for determining the effectiveness of the system of internal control within their respective units and should ask such questions as:

- Do the unit's objectives provide it with a clear direction?
- Do people in the unit understand the objectives, and how does achievement of the objectives help to accomplish the agency's mission?
- Does the control environment help to foster achievement of the unit's objectives?
- Does the unit have a means of effectively identifying and managing risk?
- Has unit management established the controls needed to minimize risk?
- Are the controls functioning as designed?
- Are the controls both effective and efficient in accomplishing their purpose?
- Does the unit receive the timely, accurate and useful information needed to achieve its objectives?
- Are communication lines sufficient to meet the needs of senders and receivers of information?
- Is monitoring within the unit effective in ensuring that daily operations are in compliance with the system of internal control?
- Is the unit effectively monitoring the accomplishment of objectives, the control environment and the communication process?
- Does monitoring adequately identify changes in the internal or external environment?
- Are existing resources sufficient to achieve program objectives in accordance with statutory and regulatory requirements?

Part II: Five Standards of Internal Control

The **Green Book** provides a framework to design, implement, and operate an internal control system and applies to all of an entity's objectives: operations, reporting, and compliance. The internal control process consists of five interrelated components that are derived from and integrated with management processes. These components define the standards for internal control and provide the basis against which internal control is to be evaluated.

Control Environment

Management and employees should establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward internal control and conscientious management.

The **control environment** sets the tone of the agency and influences the effectiveness of internal controls. The control environment is the foundation for all other components of internal control, providing discipline and structure and encompassing both technical competence and ethical commitment. If this foundation is not strong, if the control environment is not positive, the overall system of internal control will not be as effective as it should be.

Principle 1 - ***Demonstrate Commitment to Integrity and Ethical Values***: The oversight body and management should demonstrate a commitment to integrity and ethical values.

The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

* Tone at the Top

* Standards of Conduct

* Adherence to Standards of Conduct

Ethical values and integrity are key factors contributing to a positive control environment. Ethical values are the standards of behavior that form the framework for employee conduct and guide employees when making decisions. People in an agency have personal and professional integrity when they adhere to ethical values. While it is management's responsibility to establish and communicate the ethical values of the department, it is everyone's responsibility to demonstrate integrity. Management provides leadership in setting and maintaining the agency's ethical tone ("tone at the top") by:

- Providing guidance for proper behavior through policy statements, codes of conduct and by behavioral example.

- Removing or reducing temptations for unethical behavior.

- Providing opportunities for employees to report noncompliance with established standards.

Principle 2 - *Exercise Oversight Responsibility*: The oversight body should oversee the agency's internal control system.

The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

* Oversight Structure

* Oversight for the Internal Control System

* Input for Remediation of Deficiencies

The oversight body coordinates the internal control assessments and monitors the implementation of corrective action initiatives. In identifying and accepting this responsibility, the oversight body should ensure employees have the skills, knowledge, and experience necessary for their duties. The oversight body should also apply skepticism and be objective when evaluating functional management and making decisions, ensure the completion of risk assessments, and remediate identified deficiencies.

Principle 3 - *Establish Structure, Responsibility, and Authority*: Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the agency's objectives.

The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

* Organizational Structure

* Assignment of Responsibility and Delegation of Authority

* Documentation of the Internal Control System

Structure refers to management's framework for planning, leading and controlling operations to achieve the agency's objectives. The organizational structure should clearly define key areas of authority and responsibility and establish appropriate lines of reporting. An organizational chart can provide a clear picture of the functional units of an agency and the relationships among them. Management should provide policies and direct communications to ensure that employees in each unit are aware of their duties and responsibilities, understand how their individual actions interrelate and contribute to the agency's objectives, understand the authority they are delegated, and recognize how and for what they will be held accountable. Management should develop and maintain documentation of its internal control system, which will establish and communicate the who, what, where, and why of internal control execution.

Principle 4 - *Demonstrate Commitment to Competence*: Management should demonstrate a commitment to recruit, develop, and retain competent individuals.

The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

* Expectations of Competence

* Recruitment, Development, and Retention of Individuals

* Succession and Contingency Plans and Preparation

Competence is a characteristic of people who possess and maintain the skill, knowledge and ability to perform their assigned duties. Management's commitment to competence includes hiring staff with the necessary skills and knowledge and ensuring that current staff receives adequate on-going training, mentoring and supervision. Key roles in the organization should have defined succession and contingency plans so the agency can continue to achieve its objectives whether there are sudden personnel changes or just the need for training personnel for the long term replacement of critical positions.

Principle 5 - *Enforce Accountability*: Management should evaluate performance and hold individuals accountable for their internal control responsibilities.

The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

* Enforcement of Accountability

* Consideration of Excessive Pressures

Mechanisms should be established for communicating and holding individuals accountable for performing internal control responsibilities and implementing necessary corrective actions. These could include establishing specific performance measures at all levels of the agency with evaluations performed timely. Management should be mindful of excessive pressures placed on personnel, resulting in "cutting corners" to meet certain goals. Adjusting the pressures may help personnel fulfill their assigned responsibilities in accordance with the agency's standards of conduct.

Risk Assessment

Internal control should provide for an assessment of the risks that an organization faces from both external and internal sources.

A precondition to risk assessment is the establishment of clear and consistent objectives at both the organization level and at the activity (program or function) level. Risk assessment is the identification, analysis, and management of risks relevant to the achievement of the agency's mission, goals and objectives. Risks include internal and external events or circumstances that may occur and adversely affect operations. Once risks are identified, management should consider their impact (or significance), the likelihood of their occurrence, and how to manage them.

Principle 6 - *Define Objectives and Risk Tolerances*: Management should define objectives clearly to enable the identification of risks and define risk tolerances.

The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

* Definitions of Objectives:

* Definitions of Risk Tolerances

Objectives should be defined in specific and measurable terms to be easily understood by all levels of personnel and enable measurement towards achieving those objectives. Management considers external and internal requirements and expectations when defining the objectives. Objectives are classified into operations, reporting and compliance categories and should align with the mission and goals of the program and agency. Ongoing measurement provides an opportunity to revise or refine the objectives as conditions evolve.

Risk tolerances are the acceptable level of variation relative to the achievement of objectives. In setting risk tolerances, management considers the relative importance and priority of the related objectives, and aligns risk tolerances with risk appetite. Both risk appetite and risk tolerance set boundaries of how much risk an entity is prepared to accept. Risk appetite is a higher level statement that considers broadly the levels of risks that management deems acceptable while risk tolerances are narrower and set the acceptable level of variation around objectives. Operating within risk tolerances provides management greater assurance that the agency remains within its risk appetite, which, in turn, provides a higher degree of comfort that it will achieve its objectives. Depending on the category of objectives, risk tolerances may be expressed as follows:

> * Operations objectives - Level of variation in performance in relation to risk.
>
> * Nonfinancial reporting objectives - Level of precision and accuracy suitable for user needs, involving both qualitative and quantitative considerations to meet the needs of the nonfinancial report user.

* Financial reporting objectives - Judgments about materiality are made in light of surrounding circumstances, involve both qualitative and quantitative considerations, and are affected by the needs of financial report users and size or nature of a misstatement.

* Compliance objectives - Concept of risk tolerance does not apply. An agency is either compliant or not compliant.

In establishing risk tolerance, at a minimum, managers can ask the following questions:

o "What obstacles could stand in the way of achieving your objective?"

o "What can go wrong?"

o "What is the worst thing that has happened?"

o "What is the worst thing that could happen?"

o "What keeps you awake at night?"

Activities with **inherent risk** have a greater potential for loss from fraud, waste, unauthorized use, or misappropriation due to the nature of the activity or asset. Examples of situations that may involve inherent risk:

- Complexity increases the danger that a program or activity will not operate properly or comply fully with applicable regulations.

- Third party beneficiaries are more likely to fraudulently attempt to obtain benefits when those benefits are similar to cash.

- Decentralization increases the likelihood that problems will occur. However, a problem in a centralized system may be more serious than a problem in a decentralized system because if a problem does exist, it could occur throughout the entire agency.

- A prior record of control weaknesses will often indicate a higher level of risk because adverse situations tend to repeat themselves.

- Failure to remedy control weaknesses identified by auditors often result in the same weaknesses reoccurring in future years.

Principle 7 - *Identify, Analyze, and Respond to Risks*: Management should identify, analyze, and respond to risks related to achieving the defined objectives.

The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

* Identification of Risks:

* Analysis of Risks

* Response to Risks

Management should consider inherent and residual risks as a basis for identifying and analyzing risks. Inherent risks are the risks to an agency in the absence of any action to control or modify the circumstances. Residual risk is the other remaining known risks after the inherent risks have been countered, factored in, or eliminated.

After risks are identified throughout the agency, they need to be evaluated in terms of:

Likelihood - The probability that the unfavorable event would occur if there were no (or limited) internal controls to prevent or reduce the risk.

Impact (or Significance) - A measure of the magnitude of the effect to an agency if the unfavorable event were to occur.

The specific risk analysis methodology used by agencies can vary because of differences in missions and the difficulty in qualitatively and quantitatively assigning risk levels. Based on the significance of the analyzed risks, responses by management may be to accept, avoid, reduce or share them in an effort to ensure risks are within the established tolerances for each objective. Management may need to reevaluate its risk tolerance or its responses if the program is unable to provide assurance that the objectives will be achieved.

The following ratings scale can be used as a tool in analyzing these risks and also aid in proportionally responding to the risks. Below are examples of "likelihood" and "impact" scales that an agency might use to measure each risk that it identifies:

Likelihood - Simple Scale

1	Low	Very unlikely (practically impossible) to remotely possible
5	Moderate	Somewhat possible to quite possible
10	High	Very likely to virtually certain

Impact - Simple Scale

1	Low	Very small (inconsequential) to small (insignificant)
5	Moderate	Important (material) to serious (very material)
10	High	Pervasive (extremely material) to extraordinary (may threaten department's existence)

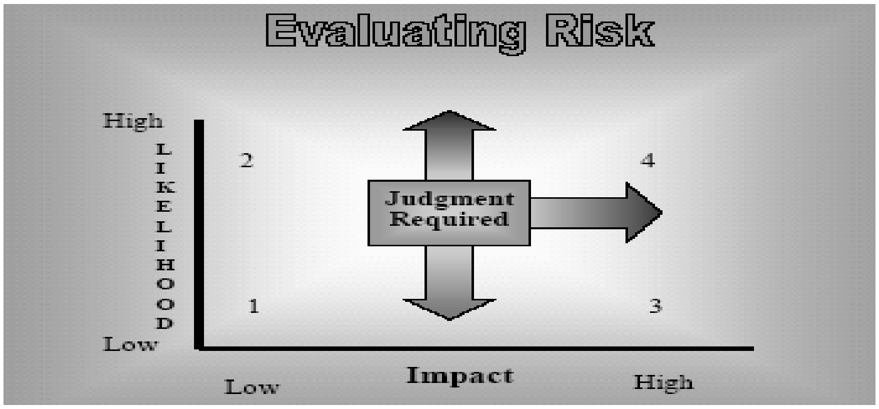
To help evaluate the risk's potential impact, agencies can consider the following list:

Impact Rating (Highest to Lowest)

- Threat to health and safety
- Long-term disruption to statewide operations
- Significant loss of revenue or assets, public distrust
- Significant disruption to operations
- Large loss of revenue or assets
- Minor disruption to operations
- Procedural issues (objectives met but could be more effective or efficient)
- Small loss of revenue or assets
- Minor errors/mistakes
- No impact

The following chart graphically depicts a reasonable approach to evaluating risks, with quadrant 1 representing the lowest priority and quadrant 4 representing the highest priority risk.

Management should use judgment to establish priorities for risks based on their impact and their likelihood of occurrence. Risks should be ranked in a logical manner, from the most significant (high impact) and most likely to occur (high likelihood) - as indicated in quadrant 4 - to the least significant (low impact) and least likely to occur (low likelihood), as indicated in quadrant 1 of the graph.



Relative Risk – An evaluation of the severity of the risk and the potential impact on operations. Items rated as “High” are considered to be of immediate concern and could cause significant operational issues if not addressed in a timely manner. Items rated as “Moderate” may also cause operational issues and do not require immediate attention, but should be addressed as soon as possible. Items rated as “Low” could escalate into operational issues, but can be addressed through the normal course of conducting business.

There are many areas of risk to consider including financial, operational, and/or compliance, to name a few. For public sector organizations, public perception should be taken into consideration when determining the relative risk rating.

Resolution Level of Difficulty – An evaluation of the estimated level of difficulty and potential cost to resolve the concern based on our experience. Items rated as “High” are considered difficult to resolve and/or will require a significant amount of planning and management involvement/oversight in order to obtain resolution. Items rated as “Moderate” are not as difficult to resolve and/or do not require a significant amount of planning, but may be time-consuming to resolve. Items rated as “Low” are items that are not complex and/or do not require significant amounts of planning and time to resolve.

Summary of Observations & Recommendations

Observations & Recommendations Summary	Relative Risk	Resolution Difficulty
1. **Observation #1**	High	Moderate
Recommendations/Corrective Actions for Observation #1		
2. **Observation #2**	High	High
Recommendations/Corrective Actions for Observation #2		
3. **Observation #3**	High	Low
Recommendations/Corrective Actions for Observation #3		

Principle 8 - *Assess Fraud Risk*: Management should consider the potential for fraud when identifying, analyzing, and responding to risks.

The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

* Types of Fraud

* Fraud Risk Factors

* Response to Fraud Risks

The types of fraud that should be considered are fraudulent financial reporting, misappropriation of assets, and corruption. In addition, other forms of misconduct, such as waste and abuse, should be considered because it could indicate potential fraud or illegal acts. Incentive/pressure, opportunity, and attitude/rationalization are all risk factors that should be considered when making assessments. Management should design an overall risk response and specific actions for responding to fraud risks. It may be possible to reduce or eliminate certain fraud risks by making changes to the agency's activities and processes. These changes may include stopping or reorganizing certain operations and reallocating roles among personnel to enhance segregation of duties. Management may also need to develop responses to address the risk of management override of controls.

Principle 9 - *Identify, Analyze, and Respond to Change*: Management should identify, analyze, and respond to significant changes that could impact the internal control system.

The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

* Identification of Change

* Analysis of and Response to Change

Any changes that could significantly impact the internal control system should be identified. Change should be part of the regular risk assessment process; however, it is discussed separately because it is critical to an effective internal control system and can be overlooked or inadequately addressed. Internal changes may include changes to the agency's programs or activities, location, oversight structure, organizational structure, personnel, or technology. External changes may include changes in governmental, economic, technological, legal, regulatory, or physical environments. Management analyzes the effect of identified changes on the internal control system and responds by revising the internal control system on a timely basis, when necessary, to maintain its effectiveness.

Control Activities

Internal control activities help ensure that management's directives are carried out. The control activities should be effective and efficient in accomplishing the agency's objectives.

Internal control activities are tools - policies, procedures, techniques, and mechanisms - that help identify, prevent or reduce the risks that can impede accomplishment of the agency's objectives. They are essential for proper stewardship and accountability of government resources and for achieving effective and efficient program results.

Control activities occur at all levels and functions of the department, including information systems. Management should establish control activities that are effective, efficient and respond to the risks. Controls need to be documented and available for review. The documentation could be in the form of management directives, agency procedures, policies or manuals.

When designing and implementing control activities, management should strive for the maximum benefit at the lowest possible cost. Here are a few simple rules to follow:

- The cost of the control activity should not exceed the cost that would be incurred by the agency if the undesirable event occurred.
- Management should build control activities into business processes and systems as the processes and systems are being designed. Adding control activities after the development of a process or system is generally more costly.
- The allocation of resources among control activities should be based on the significance and likelihood of the risk they are preventing or reducing.

Principle 10 - *Design Control Activities*: Management should design control activities to achieve objectives and respond to risks.

The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

* Response to Objectives and Risks

* Design of Appropriate Types of Control Activities

* Design of Control Activities at Various Levels

* Segregation of Duties

Management designs policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the agency's objectives and address related risks. Management also defines responsibilities, assigns them to key roles, and delegates authority to achieve the agency's objectives. As part of the risk assessment component, management identifies the risks related to the agency and its objectives; the agency's risk tolerance; and risk responses. The control activities are designed to fulfill defined responsibilities and address the identified risk responses and help management fulfill responsibilities and address identified risk responses in the internal control system. Listed below are examples of some common control activity categories that may be useful to management:

* Top-level reviews of actual performance;
* Reviews by management at the functional or activity level;
* Management of human capital;
* Controls over information processing;
* Physical control over vulnerable assets;
* Establishment and review of performance measures and indicators;
* Segregation of duties;
* Proper execution of transactions;
* Accurate and timely recording of transactions;
* Access restrictions to and accountability for resources and records;
* Appropriate documentation of transactions and internal control.

Most control activities can be grouped into the following two categories:

- **Prevention** activities are designed to deter the occurrence of an undesirable event. The development of these controls involves predicting potential problems before they occur and implementing ways to avoid them.

- **Detection** activities are designed to identify undesirable events that do occur, and alert management about what has happened. This enables management to take corrective action promptly.

No one control activity provides all of the answers to risk management problems. In some situations, a combination of control activities should be used, and in others, one control activity could substitute for another.

Management designs entity-level control activities, transaction control activities, or both depending on the level of precision needed so that the agency meets its objectives and addresses related risks. Entity-level controls are controls that have a pervasive effect on an agency's internal control system and may pertain to multiple programs or agency wide. Transaction control activities, such as SAP functionality, are actions built directly into operational processes to support the agency in achieving its objectives and addressing related risks.

Principle 11 - ***Design Activities for the Information System***: Management should design the agency's information system and related control activities to achieve objectives and respond to risks.

The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

* Design of the Agency's Information System

* Design of Appropriate Types of Control Activities

* Design of Information Technology Infrastructure

* Design of Security Management

* Design of Information Technology Acquisition, Development, and Maintenance

While some of the control activities relating to information technology (IT) are the responsibility of specialized IT personnel, other IT control activities are the responsibility of all employees who use computers in their work. For example, any employee may use: encryption tools, protocols, or similar features of software applications that protect confidential or sensitive information from unauthorized individuals; back-up and restore features of software applications that reduce the risk of lost data; virus protection software; and passwords that restrict user access to networks, data and applications.

IT control activities can be categorized as either general or application controls. General controls apply to all computerized information systems - mainframe, minicomputer, network, and end-user environments. Application controls apply to the processing of data within the application software and help ensure that transactions are valid, properly authorized and processed, and reported completely and accurately. Application controls also take into account the whole sequence of transaction processing from the preparation of the initial source document or online data entry to the creation and use of the final output. General and application controls are interrelated. General controls support the functioning of application controls, and both types of controls are needed to ensure complete and accurate information processing.

General controls include:

- Entity-wide Security Management Program: a comprehensive, high-level assessment of risks to information systems incorporating a plan that clearly describes the organization’s security management program and policies and the procedures that support it, including procedures for the secure storage and disposal of sensitive information.
- Access Controls: physical and software processes to prevent or detect unauthorized access to systems and data. These controls protect the systems from inappropriate access and unauthorized use by hackers and other trespassers or inappropriate use by agency personnel.
- Application Software Development and Change: provides the structure for the safe development of new systems and the modification of existing systems. Control activities should include system documentation requirements; authorizations for undertaking projects; and reviewing, testing, and approving development and modification activities before placing systems into operation.
- System Software Controls: the controlling and monitoring of access to use and changes made to system software, including security procedures over the acquisition, implementation, and maintenance of all system software; data-based management systems; telecommunications; security software; and utility programs.

- Segregation of Duties: Key tasks and responsibilities should be divided among various employees and sub-units of the computer operations. No one individual should control all of the primary elements of a transaction, event or process.
- Service Continuity: Maintaining or reestablishing the activities or level of service provided by an entity in the event of a disaster or other damaging occurrence. It is critical that an entity have backup and recovery procedures, and contingency and disaster plans. Data center and client-server operation controls involve steps to prevent and minimize potential damage to hardware and software and the interruption of service through the use of data and program backup procedures. (Compliance with *Management Directive 205.41, Commonwealth of Pennsylvania Continuity of Operations (COOP) Program*)

Application controls include:

- Input controls: processes for verifying data accuracy and completeness upon data-entry to a system. These controls also provide specific mechanisms for input authorization, data conversion, data editing and error handling;
- Processing controls: help ensure that data remains complete and accurate during updating, and that the application programs perform as intended;
- Output controls: help ensure that system-generated information is accurate, properly recorded, and received or reviewed by authorized individuals only. As information technologies advance and internet use increases, modifications will have to be made in each entity's specific IT control activities.

Principle 12 - *Implement Control Activities*: Management should implement control activities through policies.

The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

* Documentation of Responsibilities through Policies

* Periodic Review of Control Activities

Documentation of policies and procedures is critical to the daily operations of an agency. These documents set forth the fundamental framework and the underlying methods and processes all employees rely on to do their jobs. They provide specific direction to employees, and help form the basis used in making decisions on a daily basis. Without this framework of understanding by employees, conflict can occur, poor decisions can be made and harm can be done to the department's reputation. Further, the efficiency and effectiveness of operations can be adversely affected.

Documentation should be available for each unit for which management is responsible. The documentation should be sufficiently detailed to allow management to monitor each unit or activity.

Management should periodically review policies, procedures, and related control activities for continued relevance and effectiveness in achieving the agency's objectives or addressing related risks. If there is a significant change in an agency's process, management should review this process in a timely manner after the change to determine that the control activities are designed and implemented appropriately. Changes may occur in personnel, operational processes, or information technology and management should consider these changes in its periodic review.

Information & Communication

Information should be recorded and communicated to management and others within the organization who need it and in a form and within a time frame that enables them to carry out their internal control activities and other responsibilities.

For an agency to run and control its operations, it must have relevant, valid, reliable, and timely communications relating to internal and external events. Managers must be able to obtain reliable information to determine their risks and communicate policies and other information to those who need it.

Principle 13 - ***Use Quality Information***: Management should use quality information to achieve the agency's objectives.

The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

* Identification of Information Requirements

* Relevant Data from Reliable Sources

∗ Data Processed into Quality Information

Managers need ongoing, reliable, relevant operational and financial data from external and internal sources to determine whether they are meeting their agency’s strategic and annual performance plans and if they are meeting their goals of accountability for effective and efficient use of resources. Operating information is also needed to determine whether the agency is achieving its compliance requirements under various statutes and regulations. Financial information is needed on a day-to-day basis to make operating decisions, monitor performance, and allocate resources, and to develop financial statements for periodic external reporting. Pertinent information should be identified, captured, and distributed in a form and time frame that permits people to perform their duties efficiently. Moreover, effective management of information technology is critical to achieving useful, reliable, and accurate recording and communication of information.

Principle 14 - *Communicate Internally*: Management should internally communicate the necessary quality information to achieve the agency's objectives.

The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

* Communication throughout the Agency

* Appropriate Methods of Communication

Effective internal communications should occur in a broad sense with information flowing down, across, and up throughout the agency.

Management should establish communication channels that:

- Provide timely information;
- Inform employees of their duties and responsibilities;
- Enable the reporting of sensitive matters including fraudulent or unethical behaviors;
- Enable employees to provide suggestions for improvement of the internal control system;
- Provide the information necessary for all employees to carry out their responsibilities effectively;
- Convey top management's message that internal control responsibilities are important and should be taken seriously; and
- Convey and enable communication with external parties.

Communication is not an isolated internal control component. It affects every aspect of an agency’s operations and helps support its system of internal control. The feedback from this communication network can help management evaluate how well the various components of the system of internal control are working.

The method of communication should consider such factors as the audience to be reached, the nature and availability of the information, the cost, and the legal or regulatory requirements. The communication could be conducted via hard copy or electronic documents or face-to-face meetings.

Principle 15 - *Communicate Externally*: Management should externally communicate the necessary quality information to achieve the agency's objectives.

The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

* Communication with External Parties

* Appropriate Methods of Communication

In addition to internal communications, management should ensure there are adequate means of communicating with, and obtaining information from, external stakeholders (e.g. suppliers, contractors, grantees, regulators, external auditors, government entities, and the general public) that may have a significant impact on the agency achieving its goals.

Management both communicates and receives through reporting lines quality information with external parties to help achieve its objectives and address related risks. When external lines of communication are compromised, laws and regulations may require separate lines of communication to be established such as whistleblower and/or ethics hotlines in order to keep information confidential.

The method of communication should consider such factors as the audience to be reached, the nature and availability of the information, the cost, and the legal or regulatory requirements. The communication could be conducted via hard copy or electronic documents or face-to-face meetings.

Monitoring

Monitoring is the review of the organization's activities and transactions to assess the quality of performance over time and to determine whether controls are effective.

As mentioned in the Purpose of the Guide portion of this document, Management Directive 325.12 requires agencies to develop formal plans to monitor their internal control systems. The last two principles of the Green Book are geared toward that end. Monitoring is a basic management duty included in routine financial and program activities like ongoing supervision, reconciliations, comparisons, performance evaluations, and status reports. Internal control systems should generally be designed to ensure that ongoing monitoring occurs in the course of normal operations. Proper monitoring ensures that controls continue to be adequate and function properly.

Principle 16 - *Perform Monitoring Activities*: Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.

The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

* Establishment of a Baseline

* Internal Control System Monitoring

* Evaluation of Results

Agency internal control monitoring assesses the quality of performance over time by putting procedures in place to monitor internal control on an ongoing basis as a part of the process of carrying out its regular activities. It includes ensuring that managers know their responsibilities for internal control and control monitoring.

Management establishes a baseline to monitor the internal control system. The baseline is the current state of the internal control system compared against management's design and should incorporate deficiencies identified in the entity's internal control system. Once the baseline is established, management can use the baseline as criteria for evaluating the internal control system. The evaluation and documented results identifies internal control issues. Management will then identify changes necessary to improve the controls in order to meet the entity's objectives.

Separate evaluations can also be used to supplement monitoring, which could be in the form of self-assessments, investigations, audits or evaluations and performed by internal or external auditors or reviewers. **The Commonwealth's GAAP and/or Single Audit would not relieve the agency from their responsibilities as required in Management Directive 325.12.**

Subgrantee/Contractor Monitoring

To ensure compliance with federal, state, programmatic and contractual requirements, agencies should establish a monitoring plan and system of controls to ensure objective reviews and fiscal oversight of program funds and activities. Each agency has the primary responsibility for administering the program; conducting periodic monitoring reviews of the operations of federal and state-funded projects; and ensuring that agencies are properly using funds.
Monitoring can be conducted through multiple avenues including:

Reporting – Reviewing financial and performance reports

Site Visits – Performing site visits to review financial and programmatic records and observe operations.

Regular Contact – Regular contacts (i.e. status reports) with subgrantees and appropriate inquiries concerning program activities.

Both the financial and programmatic aspects of the grants should be reviewed closely to ensure it meets the objectives of the agreement. Monitoring should also include compliance analysis of federal and state regulations and adequately documented internal controls.

Monitoring Objectives

- To determine if grant-funded programs, and their individual activities are, carried out as described in the agreement. To determine if activities are performed in a timely manner and in accordance with the timeframe in the agreement.
- To determine if costs charged to the program are supportable, allowable, reasonable, and allocable under state and federal laws.
- To determine if activities are conducted with adequate internal control over program and financial performance, and in a way that minimizes the risk of waste, fraud and abuse.
- To ensure there is sufficient continuing capacity to carry out the approved program,
- To identify potential problem areas and to assist appropriate parties in complying with applicable laws and regulations.
- To provide adequate follow-up measures to ensure that a corrective action plan is promptly and properly implemented to correct deficiencies...
- To investigate any conflicts of interest in the operation of the program.
- To ensure that records are in compliance with program or federal requirements. This

would include, but not be limited to; any documentation to support eligibility determination, procurement procedures, expenditures and compliance with the funding source.

- To ensure that full compliance is achieved with all applicable laws, regulations, agreement terms, and fiscal oversight responsibilities.

Principle 17 - *Evaluate Issues and Remediate Deficiencies*: Management should remediate identified internal control deficiencies on a timely basis.

The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

* Reporting of Issues

* Evaluation of Issues

* Corrective Actions

Separate evaluations of internal control should be periodically performed and management should create a corrective action plan for any significant deficiencies and material weaknesses identified. This corrective action plan should be continually monitored to ensure that issues are being quickly resolved.

Glossary

Accountability: The recognition and acceptance that one is answerable for whatever happens within a particular area of activity of assigned responsibility regardless of the cause.

Component: One of five standards of internal control. The internal control components are the control environment, risk assessment, control activities, communication and information, and monitoring.

Information and Communication: The fourth component of internal control; an agency must have relevant, reliable, and timely communications relating to internal and external events.

Control Activities: The third component of internal controls; the structure, policies, and procedures, which an agency establishes so that identified risks do not prevent the agency from reaching its objectives.

Control Environment: The first component of internal controls; it sets the tone of the agency influencing the effectiveness of internal controls and is the foundation for all other components of internal control, providing discipline and structure and encompassing both technical competence and ethical commitment.

Control Objectives: The objectives of an internal control system: (1) reliable financial reporting, (2) effective and efficient operations, and (3) compliance with applicable laws and regulations.

Corruption: Bribery and other illegal acts.

COSO: The Committee of Sponsoring Organizations of the Treadway Commission. It consists of the following organizations: the American Institute of Certified Public Accountants, the American Accounting Association, the Institute of Internal Auditors, the Institute of Management Accountants, and the Financial Executives Institute.

Detective Control: A control designed to discover an unintended event or result (contrast with *Preventative Control).*

Effectiveness: The degree to which an agency or program is successful at meeting goals, objectives, and statutory mandates.

Efficiency: The degree to which an agency or program is successful at meeting goals and objectives with the least use of resources.

Fraudulent Financial Reporting: Intentional misstatements or omissions of amounts or disclosures in financial statements to deceive financial statement users. This could include intentional alteration of accounting records, misrepresentation of transactions, or intentional misapplication of accounting principles.

Goal: An elaboration of the mission statement, developed with greater specificity of how an agency will carry out its mission. The goal may be of a programmatic, policy, or fiscal nature, and is expressed in a manner that allows a future assessment to be made of whether the goal was or is being achieved.

Inherent Limitations: Those limitations of all internal control systems. The limitations relate to the limits of human judgment, resource constraints and the need to consider the cost of controls in relation to expected benefits, the reality that breakdowns can occur, the possibility of management overrides, and collusion.

Internal Control: A process, affected by an agency's oversight body, 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.

A less technical definition might define Internal Control as…

> The integration of the activities, plans, attitudes, policies, and efforts of the employees of an agency working together to provide reasonable assurance that the agency will achieve its mission.

Internal Control System: A synonym for ***Internal Control***

Management Intervention: Management's actions to override prescribed policies or procedures for legitimate purposes; management intervention is usually necessary to deal with non-recurring and non-standard transactions or events that otherwise might be handled inappropriately by the system. (Contrast this term with *Management Override.*)

Management Override: Management's overruling of prescribed policies or procedures for illegitimate purposes with the intent of personal gain or an enhanced presentation of an entity's financial condition or compliance status. (Contrast this term with Management Intervention.)

Misappropriation of Assets: Theft of an agency's assets. This could include theft of property, embezzlement of receipts, or fraudulent payments.

Mission: The fundamental purpose for which an agency exists. A *mission statement* establishes the basis for the goals of the agency by describing in broad terms what the agency intends to accomplish.

Monitoring: The fifth component of internal control, it ensures that controls are adequate and function properly.

Objective: A sub-goal identified in specific, well-defined, and measurable terms that contributes to the achievement of an agency's goal.

Oversight Body: The designated members of an agency's senior management team responsible for overseeing management's design, implementation, and operation of the internal control system.

Policy: Management's directive of what is required to effect control. A policy serves as the basis for the implementation of management directives.

Preventative Control: A control designed to avoid an unintended event or result. (Contrast with *Detective Control.*)

Procedure: An action that implements a policy.

Process: A series of activities that are linked to perform a specific objective.

Reasonable Assurance: The concept that internal control, no matter how well designed and operated, cannot guarantee an agency's objectives will be met. This is because of inherent limitations in all internal control systems.

Reliable: A high degree of certainty and predictability for a desired outcome.

Risk: Anything that endangers the achievement of an objective.

Risk Appetite: The amount of risk exposure or potential impact from an event that an agency is willing to accept or retain.

Risk Assessment: The second internal control component; the process used to identify, analyze, and manage the potential risks that could hinder or prevent an agency from achieving its objectives.

Segregation of Duties: An internal control activity to detect errors and prevent wrongful acts; it requires that different personnel perform the functions of initiation, authorization, record keeping, and custody.

Valid: Produces or relates to the intended results or goal.

Internal Control Reference Sources

Committee of Sponsoring Organizations of the Treadway Commission (COSO)
http://www.coso.org/
Internal Control – Integrated Framework

Comptroller of Maryland
http://comptroller.marylandtaxes.com/
Internal Control Manual For Use by State Departments And Independent Agencies

Massachusetts Office of the Comptroller
http://www.mass.gov/osc/overview.htm
Internal Control Guide for Managers

New York State Internal Control Association
http://www.nysica.com/

New York State Office of the State Comptroller
http://www.osc.state.ny.us/
Standards for Internal Control in New York State Government

Rhode Island
http://www.audits.ri.gov
Internal Control Guide & Resources

Vermont Department of Finance & Management
http://finance.vermont.gov/policies_procedures/internal_controls
Internal Control Standards – A Guide for Managers

U.S. Government Accountability Office
http://www.gao.gov/
Standards for Internal Control in the Federal Government