Standards for Internal Control in New York State Government

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

March 2016

A Message from State Comptroller Thomas P. DiNapoli

For over 25 years, New York State law has required State agencies and public authorities to maintain a system of internal control to help safeguard public assets and promote accountability in government. Under these same laws, the Office of the State Comptroller is responsible for developing these *Standards for Internal Control in New York State Government,* which provide a basis of common understanding and establish minimum expectations to assist public sector managers in this effort.

On the heels of the 2005 revision of the *Standards*, the New York State Internal Control Task Force—a joint effort between my office, the Division of the Budget and the New York State Internal Control Association—issued a report recommending sweeping changes in the ways the internal control and internal audit functions are managed, monitored and administered in New York State. While many recommendations required operating changes at the agency level, others called for clarification and greater specification in both the Budget regulations that govern the internal control program and in these *Standards*, against which the programs are measured. The subsequent revision of these *Standards* in 2007, incorporated many of the changes recommended by the Task Force, thereby bringing the minimum expectations for internal controls in New York State in line with the consensus opinion of the report. Six years later, in May 2013, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) presented an update to its Internal Control – Integrated Framework. This latest revision incorporates COSO's recommended changes to the Framework in order to enhance the fundamental concepts and enable New York State government organizations to effectively and efficiently develop and maintain their internal control systems.

Remember, as I have said before, internal controls are much more than just a set of procedures we put in place to safeguard assets. Rather, they are the cumulative sum of all the things we do as public servants to identify, monitor and manage risk in our organizations. This comprehensive view of risk management is critical to ensuring that New York State citizens enjoy the levels of public integrity, accountability and ethical behavior that they expect and deserve. My staff and I look forward to working with you to ensure that each of us is able to deliver on that promise.

Table of Contents

Introduction

The New York State Governmental Accountability, Audit and Internal Control Act of 1987 (Internal Control Act) required State agencies and other organizations to promote and practice good internal control and to provide accountability for their activities. In 1999, this legislation was made permanent and the State Finance Law was amended to require the State Comptroller to issue internal control standards for State agencies, public authorities and other organizations.

To fulfill this requirement, the State Comptroller developed the internal control standards contained in this publication: *Standards for Internal Control in New York State Government*. These *Standards* are based in part on the work of those advocated by leading authorities in the field of internal control, such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO), the U.S. Government Accountability Office (GAO) and other professional organizations. All organizations subject to audit by the Office of the State Comptroller, including State agencies and public authorities, are expected to adhere to these standards, and will be evaluated accordingly in any audits that are performed by that Office.

Internal control is defined as 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. It is the integration of the activities, plans, attitudes, policies, systems, resources and efforts of the people of an organization working together to achieve its mission. Thus, internal control is focused on the mission of the organization, and this mission must be kept in mind when evaluating the appropriateness of specific internal control practices.

The fundamental concepts of internal control are rooted in well-established organizational techniques and practices. The use of these techniques and practices to achieve a strong, effective system of internal control can best be understood within the following conceptual framework: the five basic components of internal control (control environment, information and communication, risk assessment, control activities, and monitoring) and the two supporting activities (strategic planning and internal audit). Each component is composed of key principles representing the fundamental concepts that are suitable for all organizations. A principle that is not present or functioning is deemed to be a "major deficiency" in internal controls. Accordingly, this publication is organized on the basis of this conceptual framework of five internal control components and seventeen related principles, together with two supporting activities.

The application of internal controls is dynamic, and practices that fit past circumstances may need to be adjusted as those circumstances change. To keep yourself informed about developments in the field of internal control and learn what other organizations are doing to meet their internal control needs, you can consult the professional literature, visit relevant websites, join professional accountability organizations, and attend training programs on the subject of internal control. Some of these potential sources of information are listed in the appendix to this publication.

Part I: New York State's Internal Control Framework

The State of New York is a very large enterprise, with an annual budget around $150 billion and a quarter million employee, as well as over 100 public authorities. It is larger than most of the Fortune 500 companies. Although governments do not seek profits, the responsibility of government officials to protect the taxpayers' money and to use public resources efficiently to serve the people is similar to the responsibility corporate executives have to their shareholders. The similarities between New York State government and big business do not end with economic comparisons. Government and many private sector companies are large organizations with many employees, multiple processes, diverse products and services and numerous customers. In order to succeed, both government and business should manage their operations effectively. While there are many different styles of effective management, there is one common feature among them: attention to internal control and risk management.

Everyone experiences internal control in their daily business activities as well as in their personal lives. Yet it is a subject that is very often misunderstood, ignored or undervalued. Internal control helps bring order, direction and consistency in daily operations and in long-term strategic planning. So, how can a subject of such importance be so unappreciated? The question underscores the need to better define internal control and what it does. This publication is intended to explain to employees of New York State government organizations how internal control plays an important part in their daily work activities.

Most people think that internal controls are about accounting for funds. While that is true, it is a myth that internal controls are only about money. Internal controls are also about demonstrating the value of an entity's programs and reporting its accomplishments. Internal controls are about protecting assets, information, and employees, and enabling the organization to make the best decisions. Internal controls are ingrained in all business systems and functions. They are essential to ensuring that an organization is functioning effectively and efficiently.

Government managers should be able not only to account for funds spent on a program, but also to assess the value of the program and measure its accomplishments. An effective system of internal control can give managers the means to provide accountability for their programs, as well as the means to obtain reasonable assurance that the programs they direct meet established goals and objectives. While managers have a significant impact on an organization's system of internal control, every employee of the organization has a responsibility and a role in ensuring that the system is effective in achieving the organization's mission.

Although an internal control system can vary widely among organizations, the standards for a good system are generally the same. The standards presented in this publication are applicable to all State government organizations, including State agencies and public authorities. You should view them as the minimally acceptable standards for New York State government organizations.

Your existing operations likely already address, at least implicitly, many of the principles and practices that are formalized in these *Standards*. You should view this information as a guide for evaluating your organization's system of internal control. More information about internal control is available in libraries, from other professional organizations and from experts on the subject, including the Office of the State Comptroller.

Definition of Internal Control

Many groups and organizations have published standards and guidelines on internal control and defined it in various ways. Each of those definitions has captured the basic concept of internal control using different words. The definitions find common ground in recognizing internal control's extensive scope, its relationship to an organization's mission, and its dependence on people in the organization.

Internal control is focused on the achievement of the organization's mission. Mission is the organization's reason for existing. It provides a sense of direction and purpose to all members of the organization, regardless of their position, and provides a guide when making critical decisions. Therefore, it is essential that an organization have a clearly stated mission that is known and understood by everyone in the organization. It is also important to understand that, while good internal control will provide "reasonable assurance" that goals and objectives are met, good internal control cannot guarantee organizational success. However, goals and objectives are much less likely to be achieved if internal control is poor.

Internal control is defined as follows:

> *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.*

In essence, internal control ensures that the right people are using the right systems to accomplish the right thing in the right way.

This definition reflects certain fundamental concepts. Internal control is:

- Geared to achieving 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 involves management and staff and the actions they take at every level in an organization, it cannot be reduced simply to policies, procedure manuals, systems, and forms. Internal control will succeed or fail depending on the attention the organization's employees give to 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 to the entire entity or to a particular subsidiary, division, operating unit, or business process.

Three Objectives of Internal Control

The overall purpose of internal control is to help an organization achieve its mission. There are three types of objectives which emphasize differing aspects 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 nonfinancial reporting. These objectives may encompass reliability, timeliness, transparency, or other terms as set forth by regulators, recognized standard setters, or the organization's policies.

- **Compliance Objectives** - dealing with adherence to laws, regulations, contracts and management directives to which the entity is subject.

Why Internal Controls are Important

Internal controls help an organization to achieve its objectives. They are the checks and balances to support the mission while helping prevent fraud, waste, and abuse and ensuring the efficient use of resources. Internal controls are the first line of defense and the best mechanism an organization has to safeguard its assets and resources, even though they can provide only reasonable—not absolute—assurance. All organizations need internal controls to:

- 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;
- Avoid bad publicity;
- Ensure public confidence; and
- Protect all employees.

Consequences of weak internal controls can range from inaccurate or incomplete information, to the waste or misuse of assets, and even to embezzlement or theft. One of the most dangerous things about a weak internal control system is that it engenders a lack of accountability. If adverse events occur, such as theft or a severe failure, it can be difficult to identify the specific cause of the problem and determine who may be responsible if accountability is not established. As a result, innocent staff can fall under suspicion. Strong controls can help to identify who or what went wrong, and what corrective actions are needed. On the broader level, a lack of accountability can result in the erosion of public confidence and support, and can also hamper an organization’s ability to serve the public effectively.

Organizational Roles

Every member of an organization has a role in the system of internal control. The human factor is critical to the system’s success. Internal controls are developed by people, guide people, and provide them with a means of accountability. People are responsible for implementing each element of the system properly. Individual roles in the system of internal control vary greatly throughout an organization. Very often, an individual's position in the organization determines the extent of that person's involvement in internal control.

The strength of the system of internal control is dependent on people's attitudes toward internal control and their attention to it. Executive management needs to set the organization’s "tone” regarding internal control. If executive management does not establish strong, clearly stated support for internal control, the organization as a whole will most likely not practice good internal control. Similarly, if individuals responsible for control activities are not attentive to their duties, the system of internal control will not be effective. People can also deliberately defeat the system of internal control. For example, a manager can override a control activity because of time constraints, or two or more employees can act together in collusion to circumvent control and "beat the system." To avoid these kinds of situations, the organization should continually monitor employee activity and emphasize the value of internal control.

While everyone in an organization has responsibility for ensuring the system of internal control is effective, the greatest amount of responsibility rests with the managers of the organization. Management has a role in making sure that all employees have the necessary skills and capacities and in providing employees with appropriate supervision, monitoring, and training to reasonably ensure that the organization has the capability to carry out its work. The organization's top executive, as the lead manager, has the ultimate responsibility. The Internal Control Act provides that the top executive is responsible for establishing the organization’s system of internal control, and is also responsible for: (1) establishing a system of internal control review; (2) making management policies and guidelines available to all employees; and (3) implementing education and training about internal control and internal control evaluations. To the extent that the top executive authorizes other managers to perform certain activities, those managers become responsible for those portions of the organization’s system of internal control.

The law further requires the head of the organization to designate an internal control officer who reports to him or her. The Internal Control Officer should be an individual with sufficient authority to act on behalf of the agency head in implementing and reviewing the agency’s internal control program. This individual should have a broad knowledge of the agency’s operations, personnel and policy objectives. Drawing on knowledge and experience with internal control matters, the internal control officer is a critical member of the management team who assists the agency head and other management officials by evaluating and improving the effectiveness of the internal control system. The Internal Control Officer is responsible for: establishing and maintaining a system of internal controls and program review; making management policies and guidelines available for all employees; and ensuring that employees have an adequate awareness and understanding of internal control standards through the implementation of education and training efforts. In general terms, the role of the Internal Control Officer is to work with appropriate personnel within the organization to coordinate the internal control activities and to ensure that the organization’s internal control program meets requirements established by law and these standards.

While the Internal Control Officer has responsibility for reviewing the organization’s internal control efforts and evaluating the adequacy of the internal control reviews, program and line managers are primarily responsible for conducting reviews to assure adherence to controls, and for analyzing and improving control systems. Ultimately, the organization’s managers are still responsible for the appropriateness of the internal control system in their areas of operation.

The Internal Control Officer helps establish specific procedures and requirements; however, the effectiveness of these procedures and requirements must be audited by someone who was not involved in the process of putting them into place. The organization's internal auditor is responsible for evaluating the effectiveness of the system of internal control, and must be independent of the activities that are audited. For this reason, in nearly all instances, the internal auditor cannot properly perform the role of Internal Control Officer.

Documentation of an Organization's Internal Control System

Documentation is a necessary part of an effective internal control system. The level and nature of the documentation required will vary, based on the size of the entity and the complexity of the operational processes the entity performs. Management uses judgment in determining the extent of documentation that is needed. Documentation is required for the effective design, implementation, and operating effectiveness of an entity's internal control system. These *Standards* includes minimum documentation requirements as follows:

- Management develops and maintains documentation of its internal control system.
- If management determines that a key internal control principle is not relevant, management supports that determination with documentation that includes the rationale of how, in the absence of that principle, the associated component could be designed, implemented, and operated effectively.
- Management documents in policies the internal control responsibilities of the organization.
- Management evaluates its operations and risks and documents its assessment of vulnerabilities.
- Management evaluates and documents the results of ongoing monitoring and separate evaluations to identify internal control issues.
- Management evaluates and documents internal control issues and determines appropriate corrective actions for internal control deficiencies on a timely basis.
- Management completes and documents corrective actions to remediate internal control deficiencies on a timely basis.

These requirements represent the minimum level of documentation of each component in an entity's internal control system. Management exercises judgment in determining what additional documentation may be necessary for an effective internal control system. If management identifies deficiencies in achieving these documentation requirements, the effect of the identified deficiencies is considered as part of management's summary determination as to whether the related principle is designed, implemented, and operating effectively.

Part II: 5 Components and 17 Principles of Internal Control

The 5 components of internal control must be successfully designed, implemented, and functioning sufficiently in order for the internal control system to be effective. The 17 principles represent the fundamental concepts which are associated with particular components within the system. All components and principles are relevant in establishing an effective internal control system. An organization that has a strong system of internal control exhibits the following actions.

Control Environment

1. **Demonstrates commitment to integrity and ethical values**
2. **Exercises oversight responsibility**
3. **Establishes structure, authority and responsibility**
4. **Demonstrates commitment to competence**
5. **Enforces accountability**

Risk Assessment

6. **Specifies suitable objectives**
7. **Identifies and analyzes risk**
8. **Assesses fraud risk**
9. **Manages risk during change**

Control Activities

10. **Selects and develops control activities**
11. **Selects and develops general controls over technology**
12. **Deploys controls through policies and procedures**

Information and Communication

13. **Uses relevant information**
14. **Communicates internally**
15. **Communicates externally**

Monitoring

16. **Conducts ongoing and/or separate evaluations**
17. **Evaluates and communicates deficiencies**

Control Environment

Control environment encompasses the set of standards, processes, and structures that are the backbone for establishing internal control across the organization. It is the attitude toward internal control established and maintained by the management and employees of an organization. It is the product of management's governance—that is, its philosophy, style and supportive attitude—and the sense of competence, ethical values, integrity and morale. The control environment is further affected by the organization's structure and accountability relationships. The control environment has a pervasive influence on the decisions and activities of an organization, and provides the foundation for the overall system of internal control. 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.

The following principles describe how management is responsible for creating a positive control environment, and how employees are responsible for helping to maintain this environment.

Demonstrates Commitment to Integrity and Ethical Values

Integrity and ethical values are key elements contributing to a good control environment. In an organizational context, ethical values are the standards of behavior that form the framework for employee conduct, guiding employees when they make decisions. Management addresses the issue of ethical values when it encourages:

- honesty and fairness;
- recognition of and adherence to laws and policies;
- respect for the organization;
- leadership by example;
- commitment to excellence;
- appropriate respect for authority;
- respect for employees' rights; and
- conformance with professional standards.

Government employees should carry out their responsibilities with exemplary integrity, commensurate with their role as public servants. While it is management's responsibility to establish and communicate the values of the organization, it is everyone's responsibility to demonstrate integrity. Management encourages integrity by:

- establishing and publishing a code of conduct;
- complying with the organization's ethical values and code of conduct;
- rewarding employee commitment to the organization's ethical values;
- establishing methods for reporting ethical violations; and
- consistently enforcing disciplinary practices for all ethical violations.

Exercises Oversight Responsibility

Governance

Governance is the influence on an organization exercised by the executive body or the chief executive. The executive body may be a board of directors, board of trustees, council, legislature or similar entity. The chief executive may be the president, chancellor, commissioner, chief judge or an individual elected or appointed as the highest ranking person in the organization.

Their governance responsibilities are usually founded in a constitution, charter, laws, by-laws, regulations and other similar documents. The leadership, actions and tone established and practiced by the governing body and/or executive can have a profound impact on how the employees of the organization perform their responsibilities, which in turn affects the achievement of the organization’s mission.

Among the critical areas influenced by the governing body or executive are:

- approving and monitoring the organization’s mission and strategic plan;
- establishing, practicing, and monitoring the organization’s values and ethical code;
- overseeing the design, implementation, and operation of the organization’s internal control system;
- providing direction to management on the correction of deficiencies in the internal control system;
- overseeing the decisions and actions of senior managers;
- establishing high-level policy and organizational structure;

- ensuring and providing accountability to stakeholders;
- establishing the overall management style, philosophy and tone; and
- directing management oversight of key business processes.

Management's Operating Style and Philosophy

Management's operating style and philosophy reflects management's basic beliefs regarding how the people and activities of an organization should be managed. There are many styles and philosophies. Although, some may be more effective than others in helping a particular organization accomplish its mission. Management should practice the most effective style and philosophy for the organization, making sure that its approach reflects the ethical values of the organization and positively affects staff morale. Management should practice and clearly communicate and demonstrate these beliefs to staff and periodically evaluate whether the style and philosophy are effective and are practiced consistently.

Management's philosophy and style can be demonstrated in such areas as: its approach to recognizing and responding to risks (both internal and external), including the potential for fraud; its acceptance of regulatory control imposed by others; its attitude toward internal and external reporting; its use of aggressive or conservative accounting principles; its attitude toward information technology and accounting functions; and its support for and responsiveness to internal and external audits and evaluations.

Supportive Attitude

A supportive attitude toward internal controls is a disposition that encourages desired outcomes. Since internal control provides management with reasonable assurance that the organization's mission is being accomplished, management should have a supportive attitude toward internal control and make sure that attitude permeates the organization. Executive management should set a tone that emphasizes the importance of internal control. Such a tone is characterized by:

- minimal and guarded use of control overrides;
- support for conducting control self-assessments and internal and external audits;
- openness and responsiveness to issues raised as the result of the evaluations and audits; and
- ongoing education to ensure everyone understands the system of internal control and their role in supporting it.

Mission

The mission of an organization should be formulated in a clear, concise statement, approved by executive management and/or the governing board of the organization. Management should tell employees about the organization's mission and explain how their jobs contribute to accomplishing the mission. The mission statement will be most effective if all employees perceive they have a personal stake in helping the organization fulfill its mission. Without a clearly defined and communicated mission, an organization may drift aimlessly and accomplish little.

As time passes, both internal and external changes can affect the organization's mission, goals and objectives. Therefore, management should periodically review the mission statement and update it, as necessary, for adequacy and relevancy.

Morale

Morale is the attitude people have about their work, as exhibited by their confidence, discipline and willingness to perform tasks. People's attitude about their jobs, work environment and organization affects how well they do their jobs. Management should recognize the importance of good morale in an effective control environment. Equally important, management should recognize that low employee morale can be detrimental to the control environment, causing a drop in productivity, turn over in key positions and lack of loyalty. Management should monitor the level of staff morale to ensure employees are committed to helping the organization accomplish its mission. Management should also take actions to maintain high morale. Such actions should provide staff with a sense that:

- their opinions and contributions are welcomed, valued and recognized;
- the organization is willing to help improve their level of competency;
- there is opportunity for continuous improvement;
- they have a stake in the mission, goals and objectives of the organization;
- the organization's appraisal and reward systems are fair and consistent;
- disciplinary actions are fair, consistently applied and timely; and
- the lines of communication are open.

Establishes Structure, Authority and Responsibility

Structure is the framework in which the organization's plans are carried out. It should define the functional subunits of an organization and the relationships among them.

An organizational chart can provide a clear picture of the authority and accountability relationships among functions. The chart should be provided to all employees to help them understand the organization as a whole, the relationships among its various components and where they fit into the organization. Management should review this chart periodically to ensure it accurately reflects the organization's structure.

Management should delegate authority and responsibility throughout the organization. Management is responsible for organizing the entity’s authority and accountability relationships among various functions to provide reasonable assurance that work activities are aligned with organizational objectives. With increased delegation of authority and responsibility, there is a need to provide qualified and continuous supervision and to monitor results. Supervision throughout the organization helps ensure that employees are aware of their duties and responsibilities, and know the extent to which they are accountable for the successful completion of specific activities.

Demonstrates Commitment to Competence

Competent employees have the skill, knowledge and ability to perform their assigned tasks. Management's responsibility for ensuring the competency of its employees should begin with establishing appropriate human resource policies and practices that reflect a commitment to:

- establishing levels of knowledge and skill required for every position;
- verifying the qualifications of job candidates;
- hiring and promoting only those with the required knowledge and skills;
- establishing training and education programs that help employees increase their knowledge and skills;
- planning and preparing for succession by developing contingency plans for the assignment of responsibilities when employees change positions or leave the organization.

Management should also ensure that employees have adequate resources, such as equipment, software, policy and procedure manuals, as well as the tools and support they need to perform their jobs.

Enforces Accountability

Management should evaluate performance and hold individuals accountable for their responsibilities in pursuit of organizational objectives. Accountability is driven by the tone at the top and supported by the commitment to integrity and ethical values. Management holds individuals accountable through mechanisms such as performance evaluations and disciplinary actions. Actions to enforce accountability for organizational responsibilities range from information feedback provided by the direct supervisor to formal disciplinary action. The level of enforcement action is determined by the significance of the deficiency to the internal control system.

Management is responsible for evaluating the pressure exerted on individuals to fulfill their assigned duties. Excessive pressure can result in individuals skipping steps or cutting corners to meet established goals. Management can adjust excessive pressures by rebalancing workloads or increasing resource levels.

Risk Assessment

Risk is the possibility that an event will occur and threaten or otherwise adversely affect the achievement of the organizations objectives. Objectives can only be derived from and must be in alignment with the organization's mission, strategic plan, and performance goals. Management should define objectives clearly to enable the identification of risks and define risk tolerances. The act of managing the risks associated with achieving an origination's mission through its objectives requires an assessment of these risks.

Risk assessment involves a dynamic and iterative process for identifying and analyzing these threats through an organization-wide effort, forming a basis for determining how risks should be managed. Management considers possible changes in the external environment and within its own business model that may impede its ability to achieve its objectives. For each risk that is identified, management should decide whether to accept the risk, reduce the risk to an acceptable level, or avoid the risk. 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.

Specifies Suitable Objectives

Objectives are driven by an organization's mission and its strategic plan, which outlines goals and priorities. Objectives detail an organization's areas of focus for accomplishing its mission and meeting its expectations. Management sets internal expectations and requirements through the established standards of conduct, oversight structure, organizational structure, and expectations of competence. Management should evaluate whether defined objectives are consistent with these requirements and expectations, and make revisions as necessary. This consistency enables management to identify and analyze risks associated with achieving the defined objectives as part of the control environment.

By stating objectives in specific and measurable terms, the design of internal control for related risks can be better understood at all levels of the organization. This involves clearly defining what is to be achieved, who is to achieve it, how it will be achieved, and the time frames for achievement. Measurable objectives are generally free of bias and do not require subjective judgment. Measurable objectives are also stated in a quantitative or qualitative form that permits reasonably consistent assessment. For quantitative objectives, performance measures may be a targeted percentage or numerical value. For qualitative objectives, management may need to design performance measures that indicate a level or degree of performance, such as milestones.

Risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. Management defines the risk tolerances for defined objectives by ensuring that the set levels of variation for performance measures are appropriate for the design of an internal control system. Risk tolerances should be measured in similar terms as the performance measures for instance, if accuracy is a measure of an objective, then risk tolerance would be stated as an acceptable error rate, note that the concept of risk tolerance does not apply to compliance, since an entity is either compliant or not compliant.

Further, management must consider the risk tolerances in the context of the entity's applicable laws, regulations, and standards as well as the entity's standards of conduct, oversight structure, organizational structure, and expectations of competence. If risk tolerances for defined objectives are not consistent with these requirements and expectations, management must make appropriate revisions to achieve consistency.

Identifies and Analyzes Risk

One of the most important components of an organization's internal control program is the process used to identify and evaluate the risks and internal controls associated with specific functions, objectives, and assessable units.

Identify Risk

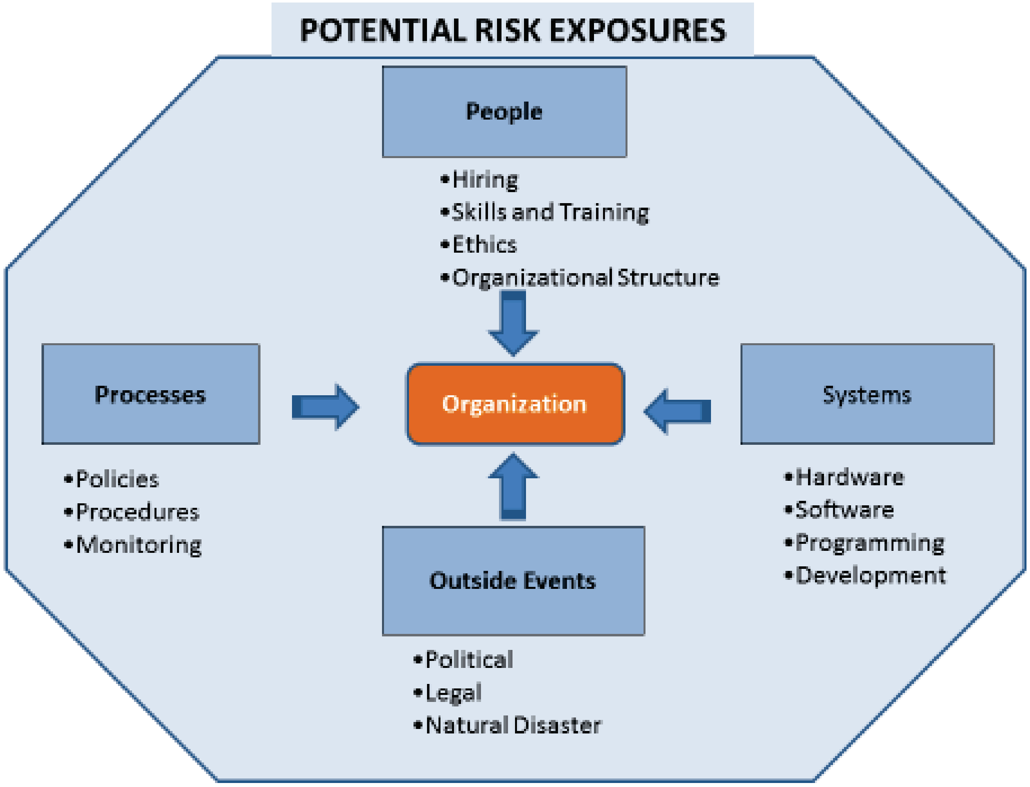
Management first needs to identify all business objectives of its programs and units, including operational goals, reporting, and compliance requirements. These objectives should be specific enough to provide direction for managing the organization's functions and should be stated in terms that reflect the responsibilities of its subunits. Business objectives should flow from the three objectives of internal control, which were discussed in Part I. For example, the following two business objectives are derived from the operational objective of internal control:

- Ensure all applications are processed (i.e., promoting the effectiveness and efficiency of the entity's operation).

- Ensure access to electronic files is restricted to authorized personnel (i.e., safeguarding assets against loss).

After identifying all the business objectives, managers should identify all the risks associated with each objective (i.e., the events that would threaten the accomplishment of each objective). These risks can be both internal (e.g., human error, fraud, system breakdowns) and external (e.g., changes in legislation, natural disasters). It is essential that managers within the organization identify the risks associated with their respective objectives. There are many ways to look at risks, and no one can identify all potential risks. One recognized approach is to conduct a group brainstorming session with staff to generate ideas on what could go wrong in an organization, operation, or unit. It's a dynamic process, allowing you to consider how potential events might affect the achievement of your objectives.

The following chart illustrates some of the places where an organization can be exposed to risk, although it is not reflective of all potential risks.



The Appendix includes references to many other resources that can help management select the most effective tools and approaches for its operations.

Information Technology Risk

As organizations continue to develop or incorporate technological advances, they become exposed to new and sometimes greater risks. Therefore, organizations must identify and assess the risks accompanying each new device, platform, software application or business model. Among the questions management should consider are:

- 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? Examples may include reduced data security, frequent or prolonged service interruptions, steep learning curves, or decreased morale.

- What changes to internal controls (e.g., control activities) are necessary to manage these risks?

Interdependencies among risks often cross business unit and functional boundaries. In recent years, government organizations have increasingly turned to third-party service providers for information technology solutions. Organizations use third parties for a variety of purposes, ranging from simple web hosting to complete outsourcing of all information technology (IT) functions. Outsourcing provides organizations with a number of benefits including the ability to utilize technology that may not otherwise be available, to access other skills and knowledge that may not exist in the organization, or to provide 24 hour-a-day, seven-day-a-week support.

The impact that third parties have on an organization can vary considerably. Third parties that provide little more than connectivity services, may have little impact on an organization's internal controls and related control objectives. Conversely, third parties that provide services ranging from application hosting to business process outsourcing to complete management of all IT-related functions can have significant impact on an organization's internal controls and related control objectives.

Regardless of the level of impact a third party can have on an organization, the governing board or organizational head and senior management are ultimately responsible for managing activities conducted through third-party relationships as well as identifying and controlling the risks arising from such relationships to the same extent as if the activity were handled within the organization. Third-party activities must be included in the organization's risk assessment, and management should implement an effective third party risk management process. Management should appropriately assess, measure, monitor, and control the risk associated with the third-party relationship. Organizations can choose to perform these assurance activities on their own or require an independent assessment of the controls around the services provided. In either situation, the organization should provide for these assurances in the agreement (contract) with the third-party and clearly state its expectations including compliance with these *Standards*. Management should consider designating a specific officer to coordinate the oversight activities and involve other operational areas in the monitoring process. An effective oversight program will generally include the monitoring of the third party's quality of service, risk management practices, and applicable internal controls.

In some instances in government operations, a third party may be another governmental entity. In those situations, wherever possible, establishing a Memorandum of Understanding (MOU) will help to clarify the requirements for both entities. Agreement on which processes each organization is responsible for, how assurances will be provided and in what format are all factors to include in such an agreement. Where an MOU does not exist, the risks associated with the outsourcing should still be recorded and tracked on a continuous basis. While it may be difficult to fully mitigate risks associated with such arrangements, it is important to inventory these risk and monitor for their occurrence with a plan for response in place should they occur.

Analyze Risk

Management should evaluate each identified risk in terms of its impact and its likelihood of occurrence, as follows:

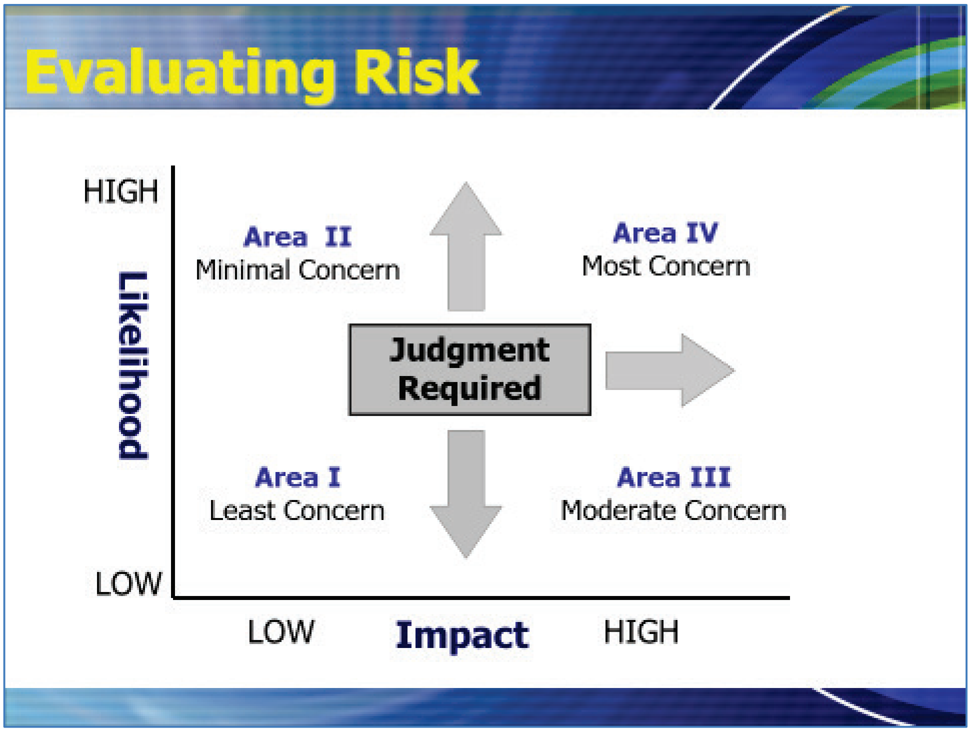
- Impact is the effect an unfavorable event would have on the organization. This effect could be some type of harm or an opportunity that would be lost. The impact is also affected by how quickly an event may happen or spread (speed) and its duration. If possible, these impacts should be quantified or, at the very least, should be described in terms that are specific enough to indicate the significance of the risk.

- Likelihood of occurrence is the probability that an unfavorable event would occur if there were no control activities (as described in the following section) to prevent or reduce the risk. A likelihood of occurrence should be estimated for each identified risk.

The combination of the two factors provides management with a rating for each risk identified. Further, management should identify the amount of risk they are willing to accept in relation to achieving objectives; thereby effectively quantifying management's tolerance for such risks.

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 those that are most significant (high impact) and most likely to occur (high likelihood) to the least significant (low impact) and least likely (low likelihood).

This chart depicts one reasonable approach that management may choose to employ to evaluating risks, where Area 1 represents the lowest priority risk and Area 4 represents the highest.



For example, a program manager may have control over two cash accounts: one, the office petty cash fund and the other, for collection of fees and fines from a program activity. Most people would likely consider the petty cash fund to be an Area 1 or 2 risk based on its small balance. In contrast, if management finds that the fees and fines are substantial in amount, are stored in an unlocked location and that there is a six-month backlog in processing them, this would likely result in an Area 4 assessment requiring immediate attention.

Risks may be analyzed on an individual basis or grouped into categories with related risks and analyzed collectively. Regardless of whether risks are analyzed individually or collectively, management should consider the correlation among different risks or groups of risks when estimating their significance. The specific risk analysis methodology used can vary by entity because of differences in missions and the difficulties inherent in qualitatively and quantitatively defining risk tolerances.

Respond to and Manage Risk

Executive management should provide guidance to managers throughout the organization to help them assess both the level and the nature of risks that and distinguish acceptable from unacceptable risks. Managers should use this guidance, along with the results of the organization's specific risk assessments, to determine actions necessary to manage each risk to an acceptable level. In each case, managers must decide whether to accept, reduce, transfer or avoid each risk entirely.

For example, in deciding how to manage the risk that unauthorized persons could gain access to electronic files, managers should consider the following possibilities:

- ***Accept the risk: Do not establish control activities*** - Management may choose to accept the risk of unauthorized access because it determines that the consequences of such access are not significant. (E.g., the files may not contain data that is sensitive.) Management might also choose to accept the risk if the cost of the associated control activities is greater than the cost of the unfavorable event.

- ***Reduce the risk: Establish control activities*** - Management cannot accept the current level of risk of unauthorized access because the files contain confidential or otherwise inherently valuable data. Therefore, management establishes control activities that are intended to reduce the risk of unauthorized access to an acceptable level. However, the risk is reduced only as long as the control activities function as intended.

- ***Transfer or share the risk*** - Management may decide to maintain electronic data in a vendor-operated cloud environment or an external data center operated by a business partner. Contract provisions may then allow management to transfer responsibility for all or part of the risk of improper access to the service provider or business partner.

- ***Avoid the risk: Do not carry out the function*** - Management determines that it cannot tolerate any risk of unauthorized access to the files or cannot adequately control such access. For example, a file may contain extremely sensitive data, or access controls may not be feasible. In this case, management may decide that the impact of any unauthorized access to this file would be too risky or that access is too difficult or too costly to control. Therefore, management decides not to carry out this function (i.e., decides not to maintain the data).

Reduce Risk

In most cases, government entities do not have the ability to eliminate programs to wholly avoid risks, and 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. Management should therefore use risk assessment information to help identify the most effective and efficient control activities available for handling the risk. Specifically, management should answer the following questions:

- ***What is the cause of the risk?*** Consider the reasons the risk exists to help identify all the possible control activities that could prevent or reduce the risk.

- ***What is the potential for fraud?*** Consider potential threats that could result in fraudulent activities.

- ***What is the cost of control vs. the cost of the unfavorable event?*** Compare the cost of the risk's impact with the cost of carrying out various control activities, and select the most cost-effective choice.

- ***What is the priority of this risk?*** Use the prioritized list of risks to help decide how to allocate resources among the various control activities used to reduce the risks. The higher the priority, the greater the resources which may be allocated to the control activities intended to reduce the risk.

Management should maintain its analysis and interpretation of the risk assessment information as part of its documentation of the rationale that supports its risk management decisions. Management should review these decisions periodically to determine whether changes in conditions warrant a different approach to managing and reducing risk.

Fraud Risk

All organizations need to consider the potential for fraud to occur in their operations. 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. Occupational fraud is the use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization’s resources or assets.

Fraud should be included as part of the risk assessment process, but can be documented separately or in conjunction with other risks. The organization should consider and assess the following when evaluating potential risks for fraud:

- **Various Types of Fraud** - fraudulent reporting, possible loss of assets, and corruption resulting from the many ways that fraud and misconduct can occur.

- **Incentives and Pressures** - internal and external motives and demands.

- **Opportunities** - vulnerabilities to unauthorized acquisition, use, or disposal of assets, altering of the entity’s reporting records, or other inappropriate acts. Also consider the opportunities for fraud and abuse afforded certain positions or scopes of authority over operations.

- **Attitudes and Rationalizations** - how management and other personnel might engage in or justify inappropriate actions.

Management analyzes and responds to identified fraud risks so that they are effectively mitigated. As part of analyzing fraud risk, management also assesses the risk of management override of controls. Management responds to fraud risks through the same risk response process performed for all analyzed risks. Management designs 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 entity's activities and processes. These changes may include stopping or reorganizing certain operations and reallocating roles among personnel to enhance segregation of duties. In addition to responding to fraud risks, management may need to develop further responses to address the risk of management override of controls.

Further, when fraud has been detected, the risk assessment process may need to be revised. In addition to fraud, management considers other forms of misconduct that can occur, such as waste and abuse. Waste is the act of using or expending resources carelessly, extravagantly, or to no purpose. Abuse involves behavior that is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary operational practice given the facts and circumstances. This includes the misuse of authority or position for personal gain or for the benefit of another. Waste and abuse do not necessarily involve fraud or illegal acts.

Manages Risk During Change

When change occurs in an organization, it often affects the control activities that were designed to prevent or reduce risk. Some examples of change include: new processes, new systems, significant changes in job responsibilities, reorganizations, significant changes in personnel, and changes in legislation. To properly manage risk, management should:

- monitor changes to ensure that each risk continues to be managed as change occurs;
- inform employees responsible for managing the organization's most critical risks about any proposed changes that may affect their ability to manage those risks; and
- continually monitor the factors that can affect the risks already identified as well as other factors that could create new risks.

Control Activities

Control activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Management should establish control activities that are effective and efficient and contribute to the mitigation of risks.

Selects and Develops Control Activities

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 organization 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 impact and likelihood of the risk they are intended to reduce.

Control activities may include a variety of approaches to mitigate risks, considering both manual and automated as well as preventive and detective controls.

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

- Detective controls are designed to identify undesirable events that do occur, and alert managers so they can take corrective action promptly.

Preventive controls can often be more expensive to operate and maintain than detective controls. Costs and benefits should be assessed before control activities are implemented. Management should also remember that an excessive use of preventive controls can impede productivity. 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. The following are descriptions of some of the more commonly used control activities. This is by no means an exhaustive listing of the alternatives available to management.

Documentation

Documentation involves preserving evidence to substantiate a decision, event, transaction or system. All documentation should be complete, accurate and recorded timely. Documentation should have a clear purpose and be in a usable format that will add to the efficiency and effectiveness of the organization. Examples of areas where documentation is important include critical decisions, significant events, transactions, policies, procedures and the system of internal control.

Critical decisions and significant events usually involve executive management. These decisions and events usually result in the use, commitment, exchange or transfer of resources, such as in strategic plans, budgets and executive policies. By recording the information related to such events, management creates an organizational history that can serve as justification for subsequent actions and decisions and will be of value during self-evaluations and audits.

Documentation of transactions should enable managers to trace each transaction from its inception through its completion. This means the entire life cycle of the transaction should be recorded, including: (1) its initiation and authorization; (2) its progress through all stages of processing; and (3) its final classification in summary records. For example, the documentation for the purchase of equipment would start with the authorized purchase request and continue with the purchase order, the vendor invoice and the final payment documentation.

Documentation of policies and procedures is critical to the daily operations of an organization. The organization deploys control activities through policies that establish what is expected and through procedures that put policies into action. 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 in their daily decision making. Without this framework of understanding by employees, conflict can occur and poor decisions can be made, causing serious harm to the organization's reputation. Further, the efficiency and effectiveness of operations can be adversely affected.

The documentation of an organization's system of internal control should include the organization's structure, policies, assessable units, control objectives and control activities. The various aspects of a system of internal control can be represented in narrative form, such as in policy and procedure manuals, and/or in the form of flow charts or matrices.

Approval and Authorization

Approval is the confirmation or sanction of employee decisions, events or transactions based on a review. Management should determine which items require approval based on the level of risk to the organization without such approval. Management should clearly document its approval requirements and ensure that employees obtain approvals in all situations where management has decided they are necessary. For example, a manager reviews a purchase request from an employee to determine whether the item is needed. Upon determining the need for the item, the manager signs the request; indicating approval of the purchase.

Authorization is the power management grants employees to carry out certain duties, based on approval received from supervisors. Authorization is a control activity designed to ensure events or transactions are initiated and executed by those designated by management. Management should ensure that the conditions and terms of authorizations are clearly documented and communicated, and that significant transactions are approved and executed only by persons acting within the scope of their authority. For example, a manager may be authorized by his or her supervisors to approve purchase requests, but only those up to a specified dollar amount.

Verification

Verification is the determination of the completeness, accuracy, authenticity and/or validity of transactions, events or information. It is a control activity that enables management to ensure activities are being done in accordance with directives. Management should determine what needs to be verified, based on the risk to the organization if there were no verification. Management should clearly communicate and document these decisions to those responsible for conducting the verifications. An example of verification is ensuring that a fair price has been obtained in a purchase and funds are available to pay for the purchase.

Supervision

Supervision is the ongoing oversight, management and guidance of an activity by designated employees to help ensure the results of the activity achieve the established objectives. Those with the responsibility for supervision should:

- monitor, review and approve, as appropriate, the work of those performing the activity to ensure the work is performed correctly;

- provide the necessary guidance and training to help minimize errors and waste and to ensure that employees understand and follow management directives; and

- clearly communicate the duties and responsibilities assigned to those performing the activities.

An example of supervision is when an assigned employee (supervisor) reviews the work of another employee processing a purchase order to determine whether it is prepared accurately and completely and has been properly authorized. The supervisor then signs the order to signify his or her review and approval. However, if there are any errors, the supervisor would return the order to the employee and explain how to complete the request properly.

Separation of Duties

Separation of duties is the division of key tasks and responsibilities among various employees and subunits of an organization. By separating key tasks and responsibilities – such as receiving, recording, depositing, securing and reconciling assets – management can reduce the risk of error, waste, or wrongful acts. The purchasing cycle is an area where the separation of duties can minimize the risk of inappropriate, unauthorized or fraudulent activities. Specifically, the various activities related to a purchase (initiation, authorization, approval, ordering, receipt, payment and record keeping) should be done by different employees or subunits of an organization. In cases where tasks cannot be effectively separated, management can substitute increased supervision as an alternative control activity that can help prevent or reduce these risks.

Safeguarding Assets

The safeguarding of assets involves restricting access to resources and information to help reduce the risk of unauthorized use or loss. Management should protect the organization's equipment, information, documents and other resources that could be wrongfully used, damaged or stolen. Management can protect these resources by limiting access to authorized individuals only. Access can be limited by various means such as locks, passwords, electronic firewalls and encryption. Management should decide which resources should be safeguarded and to what extent. Management should make this decision based on the vulnerability of the items being secured and the likelihood of loss.

Reporting

Reporting is a means of conveying information. It serves as a control when it provides information on issues such as timely achievement of goals, budget status and employee concerns. Reporting also helps to promote accountability for actions and decisions. An example of a report that serves as a control activity would be one that compares purchasing activities with the approved budget, indicating and explaining significant variances between the two.

Control Activities for Information Technology

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;
- backup 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, including mainframes, personal computers, server networks, virtual private networks and end-user environments. Application controls apply to the processing of data within the application software.

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

General controls are concentrated on six major types of control activities: an entity-wide security management program; access controls; application software development and change; system software controls; segregation of duties; and service continuity.

- An organization-wide security management program includes a comprehensive, high-level assessment of risks to information systems. An organization should have a plan that clearly describes its security management program and policies and the procedures that support it, including procedures for the secure storage and disposal of sensitive information. The organization should also establish a structure to implement and manage the security program with security responsibilities clearly defined. In addition, the organization should monitor the effectiveness of the security program and make changes as needed.

- Access security controls are 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, and form inappropriate use by agency personnel. Specific control activities may include:

    - restrictions on users allowing access only to the system functions they need to perform their assigned duties;

    - software and hardware firewalls to restrict access to assets, computers, and networks by external persons; and
    - frequent changes of passwords and deactivation of former employees' passwords.

- Application software development and change control 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 control is 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.

- The concept of segregation of duties in a computer environment is the same as in a manual process. Key tasks and responsibilities should be divided among various employees and subunits of the computer operations. No one individual should control all of the primary elements of a transaction, event or process. Identifying incompatible duties and implementing policies to separate those duties can be monitored through the use of access controls as well as by implementing operating procedures, supervision, and the review of employee activities.

- Service continuity is concerned with maintaining or re-establishing the activities or level of service provided by an organization in the event of a disaster or other damaging occurrence. It is critical that an organization 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. Such procedures include: off-site storage of backup data; environmental controls; staff training; and hardware maintenance and management. Organizations should develop, document and periodically test their contingency plans.

Application Controls

Application controls help ensure that transactions are valid, properly authorized, and processed and reported completely and accurately. These 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. As such, application controls consist of input, processing, and output controls:

- Input controls include 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 organization's specific IT control activities. However, the basic requirements of control will not change. As more powerful computers place more responsibility for data processing in the hands of the end users and as Internet use grows, organizations must be prepared to implement the controls necessary to maintain an effective system of internal control.

This information is not meant to be a complete explanation of all IT control activities. Additional guidance has been issued by the New York Office of Information Technology Services. Further guidance can also be obtained from sources such as ISACA's *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT* and the National Institute of Standards and Technology's special publications.

Deploys Controls Through Policies and Procedures

Management documents, in policies, the internal control responsibilities of the organization. This documentation generally consists of the following:

- each unit's responsibility for an operation process's objectives and related risks;

- control activity design;

- implementation; and

- operating effectiveness.

Individuals in key internal control roles may further define policies for day-to-day procedures depending on the propensity for change in the environment and the complexity of the process. Policies should be communicated and available to employees in accordance with their duties, and management should ensure employees understand their responsibilities related to policies affecting their functions. Further, management should periodically and systematically review policies, procedures and related control activities for relevance and effectiveness in achieving objectives and addressing related risks.

Information and Communication

Information is necessary for the organization to carry out internal control responsibilities to support the achievement of its objectives. Management obtains or generates and uses relevant and high quality information from both internal and external sources, as well as providing communication internally and externally to support the functioning of other components of internal control.

Uses Relevant Information

Management uses relevant and high quality information to make informed decisions and evaluate the organization's performance in achieving key objectives and addressing risks. For information to be relevant, it must come from reliable internal and external sources in a timely manner based on the identified information requirements. Quality information must be appropriate, current, complete, accurate, accessible, and provided on a timely basis.

Communicates Internally

Internal communication is the continual, iterative process of obtaining, providing, and sharing necessary information. Information should be communicated to management and other employees who need it in a form and within a time frame that helps them to carry out their responsibilities. It enables personnel to receive a clear message from senior management that control responsibilities must be taken seriously.

Information can be communicated verbally, in writing and electronically. While verbal communication may be sufficient for many day-to-day activities, it is best to document important information. This provides a more permanent record and enables managers and others to review the information.

Information should travel in all directions (across, up and down an organization) to ensure that all members of the organization are informed and that decisions and actions of different units are communicated and coordinated. A good system of communication is essential for an organization to maintain an effective system of internal control. A communication system consists of methods and records established to identify, capture and exchange useful information. Information is only useful when it is timely, sufficiently detailed and appropriate to the user.

Management should establish communication channels that:

- provide timely information;
- can be tailored to individual needs;
- inform employees of their duties and responsibilities;
- enable the reporting of sensitive matters;
- enable employees to provide suggestions for improvement;
- provide the information necessary for all employees to carry out their responsibilities effectively; and
- convey top management's message that internal control responsibilities are important and should be taken seriously.

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

Communicates Externally

External communication with customers, suppliers, regulators and other outside parties is also essential to effective internal control. Information should be communicated externally through appropriate reporting lines so that external parties can help the entity achieve its objectives and address related risks.

Management should establish separate reporting lines that:

- allow for whistleblower and ethics hotlines for communicating confidential information;
- inform external parties of these separate reporting lines;

- educate the public and employees as to how these reporting lines operate;
- convey how these reporting lines are to be used; and
- instruct how the information will remain confidential.

External information can also be communicated verbally, in writing and electronically. Management considers a variety of factors when selecting an appropriate method of communication including its audience, nature of information provided, availability, cost, and legal or regulatory requirements.

MONITORING

Conducts Ongoing and/or Separate Evaluations

Monitoring is the ongoing evaluation of internal control components, either individually or as a whole system, to ascertain whether they are present and functioning. Management should focus monitoring efforts on internal control and achievement of the organization’s mission.

Everyone within an organization has some responsibility for monitoring. The position a person holds in the organization helps to determine the focus and extent of these responsibilities. Therefore, the monitoring performed by staff, supervisors, mid-level managers and executives will not have the same focus, as follows:

- **Staff -** The primary focus of staff members should be on monitoring their own work to ensure it is being done properly. They should correct the errors they identify before work is referred to higher levels for review. Management should educate staff regarding control activities and encourage them to be alert to and report any irregularities. Because of their involvement with the details of the organization's daily operations, staff members have has the best vantage point for detecting any problems with existing control activities. Management should also remind staff to note changes in their immediate internal and external environments, to identify any risks and to report opportunities for improvement.

- **Supervisors -** Supervision is a key element of monitoring. Supervisors should monitor all activities and transactions in their unit to ensure that staff members are performing their assigned responsibilities, control activities are functioning properly, the unit is accomplishing its goals, the unit's control environment is appropriate, communication is open and sufficient, and risks and opportunities are identified and properly addressed.

- **Mid-Level Managers -** Mid-level managers should assess how well controls are functioning in multiple units within an organization, and how well supervisors are monitoring their respective units. The focus of these managers should be similar to that of supervisors, but should extend to cover all the units for which they are responsible.

- **Executive Management -** Executive management should focus their monitoring activities on the major divisions of the organization. Because of this broader focus, executive managers should place even more emphasis on monitoring the achievement of the organization's goals. Executive managers should also monitor for the existence of risks and opportunities in either the internal or external environment that might indicate the need for a change in the organization's plans.

Management should ensure that it takes the proper actions to address the results of monitoring. For example, management may decide to establish new goals and objectives to take advantage of newly identified opportunities, may counsel and retrain staff to correct procedural errors or may adjust control activities to minimize risk in response to changed circumstances. Further, independent evaluations should be performed periodically to provide objective feedback.

The monitoring performed by staff, supervisors, mid-level managers and executives should focus on the following major areas:

- **Control Activities -** Control activities are established to prevent or reduce the risk of an unfavorable event from occurring. If these activities fail, the organization becomes exposed to risk. Control activities can fail when controls are overridden, or when there is collusion for fraudulent purposes. Therefore, management should establish procedures to monitor the functioning of control activities and the use of control overrides. Management should also be alert to signs of collusion. Effective monitoring gives management the opportunity to correct any control activity problems and to control the risk before an unfavorable event occurs.

- **Mission -** Monitoring activities should include the development and review of operational data that would allow management to determine whether the organization is fulfilling its mission. This can be achieved by periodic comparison of operational data to the organization’s strategic plan.

- **Control Environment -** Executive management should monitor the control environment to ensure that managers at all levels are maintaining established ethical standards of behavior and that staff morale is at an appropriate level. Managers should also ensure that the staff is competent, that training is sufficient and that management style and philosophy foster the accomplishment of the organization's mission.

- **Information and Communication -** Managers should periodically verify that the employees they are responsible for are receiving and sharing information appropriately, and that this information is timely, sufficient and appropriate for the users. Management should ensure that there are open lines of communication, which fosters reporting of both positive and negative results.

- **Risks and Opportunities -** Managers should also monitor the organization's internal and external environment to identify any changes in risks and the development of opportunities for improvement. If changes are identified, managers should take appropriate action to address these new or changed risks and opportunities. Management should recognize that delays in responding to risks could result in damage to the organization, and a missed opportunity may result in a loss of new revenue or savings.

Evaluates and Communicates Deficiencies

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. For monitoring to be most effective, all employees need to understand the organization's mission, objectives, and risk tolerance levels as well as their own responsibilities. (See Part III for further details on evaluation).

Part III: Managing and Evaluating the Internal Control System

These *Standards* are not intended to dictate a specific structure for managing and evaluating a system of internal control in New York State government operations. That being said, there are common attributes present among operations that have strong systems of internal control. This section highlights the elements common to successful systems of internal control.

Responsibility for Managing the System

This may come as a surprise to some readers, but 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 for purposes of issuing financial statements. 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. 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.

If an entity has a governing board, that board’s responsibilities for internal controls primarily involve oversight, authorization and ethical leadership. If an entity does not have a governing board, this overarching responsibility falls to the head of the organization (e.g., Commissioner, Executive Director). Generally, governing boards or organizational heads do not design internal controls or prepare the written policies they adopt. Instead, the governing board relies upon management, especially the executive operational head (e.g., Executive Deputy, Deputy Director), to create the policies needed to ensure that the organization accomplishes its mission. Executive management in turn relies upon managers and department heads to recommend and implement procedures that lower identified risks. Wherever the responsibility for final approval of policies and procedures lies, this group or individual should take great care in reviewing these directives to ensure they are addressing risk appropriately.

Within the managerial ranks, the executive operational head provides the leadership needed to establish and guide an integrated internal control framework. This individual must establish a positive “tone at the top” by conducting the organization’s affairs in an honest and ethical manner and by establishing accountability at all levels of the organization. If the executive operational head does not demonstrate strong support for internal controls, the organization as a whole will be unlikely to practice good internal controls.

While the executive operational head is responsible for the design and maintenance of the entity's control framework, the operational managers and department heads are the front line for implementing and monitoring internal controls. These individuals are responsible for supporting the internal control initiatives of the board and/or organizational and operational heads of the organization in daily operations. All levels of management must work together to create an integrated framework that lowers risk to an acceptable level and assists the organization in meeting its goals and objectives. Managers and department heads are generally responsible for identifying potential risks, designing and implementing controls for their areas of responsibility, and keeping current with events and changes that may affect the controls they have put into place.

The Importance of Internal Control and Risk Management

For New York State government operations, compliance with the spirit of the Internal Control Act will go a long way toward realizing the benefits of effective internal control and risk management. Compliance is best accomplished by having a system of internal control whose principal aim is to manage risks that threaten the achievement of an organization's objectives. This entails not only performing risk assessments as discussed in the previous section of these *Standards*, but also:

- Identifying the organization's risk tolerance (e.g., margin of error, materiality) and what is deemed an unacceptable event;

- Monitoring legislation, market conditions, or political changes and their resulting potential impact on the organization on an ongoing basis; and

- Performing internal assessments of entity-wide risk, both actual and potential, with mitigation strategies.

An annual evaluation, although helpful, should not be the only occasion for risk assessment and monitoring. To ensure that the right controls are in place, it is best to build risk assessment and monitoring into ongoing management processes. Risks facing organizations are continually changing, and a successful system of internal control must be responsive to such changes, enabling adaptation. Effective risk management and internal control are therefore reliant on a regular evaluation of the nature and extent of risks.

In summary, to achieve a strong system of internal control, an organization needs to establish a clear link to risk management. This promotes the most effective and efficient combination of controls necessary to ensure that organizational objectives can be achieved.

Managing the Internal Control System

While the governing body or the head of the organization is responsible for ensuring an adequate internal control system is in place, 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. Many organizations have established a distinct internal control or risk management function responsible for assessing the risks to the organization and the control system's adequacy in addressing these risks.

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. While monitoring these risks and continually reviewing the organization's environment for changes that could impact its mission is an ongoing process, a formal assessment of all inherently high-risk functions should occur at least annually, and lower risk categories should be reviewed at least every three years. The formal report of deficiencies should be directed to the governing body or head of the agency and the audit committee, if one exists. Further, the Internal Control Officer –or in some entities, the Chief Risk Officer – should present enterprise risks based on analysis of reported deficiencies and appropriate review of the internal and external environmental monitoring.

Some organizations also use a senior-level risk management committee, usually consisting of the Internal Control Officer and executives charged with other functions that routinely deal with enterprise risk and risk mitigation (e.g., Counsel, Information Security Officer, etc.). Further enhancement to a risk committee would ideally include key business unit leaders to ensure that the organization's risk efforts are firmly embedded within core business activities. This group may have many responsibilities that range from establishing consistent risk definitions and terminologies, to reviewing reported deficiencies for completeness, and evaluating trend indicators and organizational risk ratings across the organization. In addition, risk management committees may also:

- **Advise on risk strategy**: The risk committee serves as a repository of information and expertise on risk and risk strategy. Thus, the risk committee can help inform the organization of risk exposures and advise on future risk mitigation efforts.

- **Assist with identifying risk appetite and tolerance**: The risk committee can help establish, communicate, and monitor the risk culture, risk appetite, risk tolerances, and risk utilization of the organization at the enterprise and business-unit levels.

- **Oversee risk exposures**: The risk committee should be continuously aware of the critical risks and exposures facing the organization and of management's strategy for addressing them. The committee should consider the full range of risks and potential interactions among risks, including risk concentrations, escalating and de-escalating risks, contingent risks, and inherent and residual risk.

- **Review crisis management plans**: The risk committee should keep abreast of the organization's crisis preparedness and ensure that management has developed and can implement a plan to respond to major risks, such as natural disasters, terrorism, cyber-attacks, epidemics, civil disorder, and other events that could compromise the enterprise's human or other resources or disrupt the value chain.

- **Support the internal control program**: The risk committee can help ensure that the Internal Control Officer has the skills, authority, and resources to oversee risk in the enterprise. The committee can also support the internal control program through consistent communications and actions regarding the organization's approach to risk and risk management.

Whoever is charged with managing and assessing the system of control must understand the nature and context of control, including an understanding of the following:

- **The system of internal control should be embedded in the operations of the organization and form part of its culture.**

  Control is affected by people throughout the organization, including the governing body, organizational head, management and all other staff. People who are accountable, as individuals or teams, for achieving objectives should also be accountable for the effectiveness of controls that support the achievement of those objectives. It is important that criteria are in place by which the effectiveness of the system of control can be judged. By making individuals accountable, the likelihood that controls will be operated properly is increased.

- **Controls should be capable of responding quickly to evolving risks, both internal and external.**

  Risks include not only those related to the achievement of a specific objective but also those fundamental to the viability and success of the organization, such as failure to maintain the organization's resilience or capacity to identify and exploit opportunities. Resilience refers to the organization's capacity to respond and adapt to unexpected risks and opportunities, and to make decisions on the basis of telltale indicators in the absence of definitive information.

- **The costs of internal controls must be balanced against the benefits, including the risks they are designed to manage.**

  Design decisions involve the acceptance of some degree of risk. The costs of control must always be balanced against the benefits of controlling the risk. It is possible to reach a position where the incremental cost of additional control is greater than the benefit derived from controlling the risk.

- **The system of internal 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 the corrective action being undertaken.**

  It should not be assumed, without making appropriate inquiries, that breakdowns in internal controls are isolated occurrences. The key is continual learning rather than attribution of blame. This philosophy should come down from the top of the company. A blame culture encourages the concealment of breakdowns in control. Often, major disasters are the result of the accumulation of a number of smaller, seemingly insignificant events, which if analyzed collectively would have provided the necessary warnings to enable preventive action.

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

  Human fallibility and the risk of unforeseeable occurrences are inherent limitations in any system of internal control. A control system cannot be designed to provide protection with certainty against an organization failing to meet its objectives or against all material errors, losses, frauds or breaches of laws or regulations.

Evaluation

Evaluation is the process management uses to determine whether**:**

- the organization will likely achieve its goals and objectives;

- the elements of the organization's internal control system are functioning effectively; and

- risks to the organization and opportunities for improvement are being identified.

It is important to note the distinction between evaluation and monitoring. Monitoring involves performing daily or routine procedures − like supervision, transaction review and problem resolution − that help to ensure operations are in compliance with the organization's system of internal control. Evaluation, on the other hand, involves conducting periodic assessments of the organization's performance compared with established expectations or measurement standards. In New York State government, this usually occurs during the annual certification process for many organizations, but should occur even if an organization is not subject to the Division of the Budget's *Budget Policy and Reporting Manual* Item B-350, entitled "Government Internal Control and Internal Audit Requirements."

Evaluation can be accomplished through self-assessment and independent review. Regular self-assessment helps management detect problems early, and thus minimizes the costs of these problems. Self-assessments should be scheduled regularly, and should be performed throughout the organization. Self-assessments can include surveys, questionnaires, interviews, observation and specific testing of transactions and key controls. Self-assessments should not only address specific processes, but also evaluate the unit's control environment, communication, monitoring and risk assessment processes.

The frequency of self-assessment should be based, in part, on the results of the organization's risk assessment process. Independent reviews can be performed by external auditors, consultants, and internal auditors who are independent of the operations to be reviewed. Such reviews should not be a substitute for routine self-assessments, but should serve to supplement them.

To perform an orderly, systematic evaluation of an organization's system of internal control, management should segment the organization into "assessable units." Assessable units are not usually the functional subunits found on an organization chart (e.g., bureaus), but are segments of them. For example, a bureau may have five or more assessable units in it, each of which performs a distinct function, program or process.

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.

Management should maintain an inventory of the assessable units along with the purpose and objectives of each assessable unit, and use it when planning any review of the system of internal control.

The managers of the assessable units should have the responsibility for determining the effectiveness of the system of internal control within their respective units. Managers should ask such questions as:

- Do the unit's objectives provide it with a clear direction?
- Do employees in the unit understand the objectives, and how achievement of the objectives helps to accomplish the organization'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?

Management should assess accomplishment of the mission at all levels of the organization on a regular basis. At production or operational levels, management should compare the actual accomplishments of the specific subunits with their operational plans and objectives, as well as, comparing the actual accomplishments of the major organizational divisions with strategic plans and organizational objectives. In addition, any new risks or opportunities that are identified in the assessment process may result in changes to the organization's objectives or modification of its mission.

All aspects of the self-assessment process should be documented, including the evaluation methodologies, the sources and types of information used, reporting relationships, any deficiencies identified, and any corrective action recommended. The results of the assessment should be communicated throughout the organization, and management should have processes in place to ensure that appropriate and prompt actions are taken to address any deficiencies identified. Management should include a review of these corrective actions in a subsequent evaluation process to determine if they have produced the desired outcomes.

Part IV: Supporting Activities

Strategic planning and internal audit are activities that support a good system of internal control. They provide management with additional tools to help ensure that the mission of the organization will be achieved.

Strategic Planning

Strategic plans are proposed courses of action designed to enable an organization to achieve its objectives and goals. Planning should begin at the top levels of management with a strategic plan that focuses on the long-range direction of the organization. The strategic planning process should include establishing the organization's broad organizational objectives and developing the strategies that should be followed to achieve them. On the basis of the direction in the organization's strategic plan, management should develop plans for each major organizational division with a long-range focus specific to that division. The division plans guide managers in developing shorter-range operational plans for each of the major functions performed within their respective divisions.

Objectives

Internal controls need to be tied to specific objectives related to reporting, compliance or operations. Strategic planning helps to define management’s organizational and operational objectives. Management derives organizational objectives from the mission and often develops them during the strategic planning process. They are long-range, broad statements that define the desired outcomes of the organization as a whole. Organizational objectives are necessary for coordinating efforts and evaluating overall performance within an organization. Without these clearly defined objectives, employees could be working inefficiently, ineffectively and/or in conflicting directions.

Good organizational objectives can serve as starting points for more specific and detailed operational objectives within the subunits (i.e., divisions, departments, bureaus and assessable units) of the organization. Operational objectives are shorter range and more specific and define the desired outcomes of each of the organization's subunits. They should be structured in a hierarchy so that each subunit's accomplishment of its operational objectives helps the next higher level achieve its operational objectives, all of which helps management meet its organizational objectives.

All objectives should be in writing. Management should provide employees with written organizational and operational objectives along with the mission statement. Management should ensure that employees understand the objectives and how their work helps to achieve them.

Finally, just as changes in the environment can affect the adequacy and relevancy of the mission statement, these same factors can also affect an organization's objectives. For an organization to function effectively and adapt, it should periodically reassess its organizational and operational objectives.

Goals

Goals are objectives translated into specific, measurable targets. They are quantifiable and provide a means for assessing the accomplishment of objectives. Management should translate all objectives into attainable goals. Progress toward these goals can help measure accomplishment of an objective. Sometimes it is difficult to translate an objective into a quantifiable goal. In such instances, management should identify some other appropriate indirect measure.

Operational Plans

Managers at all levels should be able to use operational plans to determine the priority and timing of objectives, to resolve conflicts between objectives, to establish the organization's policies and procedures, and to help set budgets, schedules and resource assignments. Planning should be based on the most objective and accurate information available. All planning processes should identify the most efficient alternatives available for accomplishing the objectives. The plans should be provided to and understood by everyone who must follow them. Management should also establish a process that identifies how and when plans should be changed to reflect both changing conditions and the availability of more accurate information. Plans should be flexible enough to allow for such changes.

Internal Audit

Internal audit functions add value to an organization’s internal control system by bringing a systematic, disciplined approach to the evaluation of risk and by making recommendations to increase the effectiveness of risk management efforts, improve the internal control structure and promote good corporate governance. The Legislature, in passing the Internal Control Act, recognized the internal audit function’s key role in supporting the internal control system and, as such, made the Division of the Budget responsible for designating which State agencies would be required to maintain internal audit units. The Division of the Budget makes this determination based in part on the size, nature and/or complexity of agency operations. Other entities may choose to establish an internal audit function as part of their management of risks and resources.

In either case, the Internal Control Act requires that these units be organized and operated in accordance with professional audit standards, in particular *The Standards for the Professional Practice of Internal Auditing* promulgated by the Institute of Internal Auditors. This section, with consideration of the recommendations promulgated in 2006 by the New York State Internal Control Task Force, further interprets those standards as they apply to New York State entities and as such, forms the minimum expectations for the organization and operation of internal audit units within New York State government. Other organizational aspects related to the formation of an internal audit unit, including minimum qualifications for internal audit directors, are addressed by the Division of the Budget in Item B-350 of its *Budget Policy and Reporting Manual.*

Auditor Independence and Compatibility with Other Duties

A major underlying principle of professional audit standards is that the internal audit function must be organizationally independent of other business activities and free from interference in establishing the scope of its work and the communication of results. This organizational alignment promotes objectivity and allows the auditor to maintain an impartial, unbiased attitude while avoiding conflicts of interest. Internal audit independence and objectivity are important to credibility and are hallmarks of executive management's commitment to promoting a strong, introspective approach to governance. Executive managers, audit committees and third parties need to know that they can rely upon the internal auditor's independence when considering his or her findings and recommendations.

To ensure independence and objectivity, the internal audit function should report to the highest level of governing body charged with the responsibility to direct and/or oversee the activities and management of the organization. Ideally then, the function should be organized under the chief executive and report directly to any audit committee, board of directors or other governing authority that may exist.

Auditor independence also entails refraining from duties that are incompatible with the objective appraisal of operations. Internal auditors should therefore avoid assuming operational responsibilities or engaging in other activities that may impair their independence, including functioning as their entity's Internal Control Officer (ICO). On the most basic level, the ICO duties are defined as working with appropriate agency personnel to coordinate the internal control activities, and to ensure that the agency's internal control program meets the requirements established in agency policy. The ICO role is therefore a management function that requires decisions about the overall design and implementation of the internal control system; as such, it is generally incompatible with the role of the internal auditor. Similarly, internal auditors should also avoid functioning as their entity's Information Security Officer (ISO), as this role not only requires specialized expertise, but can also require the auditor to perform management functions or make management-level decisions.

Although it is critical for agencies and other government organizations to preserve the independence of their internal audit operations, as a practical matter, some may experience temporary situations whereby they have insufficient resources to fully separate internal audit from their internal control and information security functions. In these situations, the internal auditor should limit his/her role to the extent possible, being careful to avoid decision making in areas such as the specific type of controls needed or the quality of controls in place. For example, if the internal auditor undertakes any internal control responsibilities, executive management needs to clearly reinforce that agency managers are the individuals responsible for maintaining an appropriate system of internal controls. Further, the agency's annual internal control certification, as well as any subsequent audits of the internal control system, should each fully disclose the internal auditor's role in the internal control process.

Separation of the internal control and internal audit functions does not preclude a strong working relationship that can create synergies between the two activities. Creating a sense of cooperation between the internal control and internal audit functions will improve the overall internal control culture of an agency. The internal control and internal audit functions reinforce one another when:

- The internal auditor uses internal control reports when planning audits;

- The auditor consistently evaluates and reports on compliance with internal control requirements in audit reports, as part of the auditor's assessment of internal controls;

- The ICO reviews internal audit reports on a regular basis to ensure that agency managers incorporate significant risks, findings and recommendations into the internal control system; and

- Follow-up audits address whether significant risks, findings and recommendations have been addressed and incorporated into the agency's internal control system.

Adopting these steps will provide the internal auditor and ICO with continuous feedback on the quality of the internal control system and, as a result, lower the risk that the system may be ineffective or lose its effectiveness over time.

Maintenance of auditor objectivity also requires a continuing assessment of each auditor's relationship with the operations she or he audits. Internal audit units therefore need to establish procedures to identify personal impairments, and should obtain information concerning potential conflicts of interest and bias from audit staff at least annually. Auditors should also immediately report any new impairment that arises to their internal audit director.

Risk-Based Audit Planning

Internal audit units exist in New York State due in major part to the provisions of the Internal Control Act, which focuses largely on control systems internal to the entity. In fact, the Act specifically requires that the internal audit function shall evaluate the agency's internal controls and operations. To fulfill this responsibility, internal audit units must devote resources to examining their organizations' internal operations and cannot simply audit outside parties that conduct business with their organizations, such as contractors, grantees or service providers. Still, the Act does not specify the minimum level of audit resources that must be devoted to internal activities, and there is no expectation that all internal audit resources be directed internally. Rather, the appropriate allocation is best determined as part of a larger analysis of risks facing the particular entity.

The Director of Internal Audit in each State agency also must periodically develop a risk-based plan of audit engagements to determine the priorities for the internal audit activity. This audit plan must be based on a risk assessment, which is updated at least annually. As part of this assessment, the internal audit unit should review and test documentation maintained by the agency's Internal Control Officer in support of the entity's annual certification. Depending on the results of these tests, the internal audit unit may be able to form a basis to rely on the certification or may decide to set it aside and conduct its own separate review of internal controls. When audits of internal control systems are performed, the auditor should identify the specific objectives of the examination and should consider examining each of the five elements of internal control along with their related principles as discussed in these *Standards*: control environment, risk assessment, control activities, information and communication, and monitoring. Depending on the needs of the agency, the audit unit may need to expand the scope of its inquiry even further.

Input from senior management and the governing board (where applicable) must also be considered in the audit planning process to ensure the plan of engagements is consistent with the organization's goals. Further, the auditor should share information and coordinate activities with other internal and external providers of relevant assurance and consulting services, both to ensure proper coverage and to minimize duplication of efforts. The Director of Internal Audit should communicate the audit plan and the associated resource requirements, including any significant interim changes, to senior management and to the board for review and approval. The Director of Internal Audit should also communicate the impact of any resource limitations and should ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.

Continuing Professional Education

To be effective in a changing world, all audit staff need to maintain and enhance their technical competence through a program of continuing education. Professional audit standards, as well as various professional licensing programs including the Certified Internal Auditor and the Certified Public Accountant, all include periodic continuing education requirements. The Internal Control Task Force report provides an extensive discussion on the need for continuing education and training of the State's internal auditors. The consensus recommendation is that each auditor is required to obtain at least 80 hours of continuing professional education every two years, with not less than 20 hours obtained during any single year. This requirement is consistent with the level of training required of other professionals conducting audits of government programs. The Task Force report appendix entitled *Guidance on Continuing Education Requirements for New York State Internal Auditors* provides a more detailed discussion of these requirements, and is incorporated by reference as part of these *Standards.*

Communication

Communication is also a critical factor in ensuring that internal audit operations provide maximum value to the organization. Professional standards require periodic meetings between the internal auditor, executive management and any governing board or audit committee that may exist. These meetings are essential to ensure the independence, effectiveness and accountability of the internal audit activity and should be held at least quarterly. The timely distribution of internal audit reports is another integral way that communication supports the independence, effectiveness and credibility of the internal audit organization. Distributing the audit reports to all stakeholders, including executive management, provides reasonable assurance that the agency will take action on the findings and recommendations contained therein. The internal audit director should be responsible for the distribution of each audit report and should provide copies to the agency head, the deputy head, the internal control officer, the audit committee (if applicable) and the head of the audited operation. Any further distribution of audit reports should be made only with the knowledge and permission of executive management.

Monitoring Audit Findings

The Internal Control Act requires internal auditors to identify internal control weaknesses that have not been corrected and make recommendations to correct those weaknesses. To accomplish this, each unit needs to establish and maintain a system to monitor the disposition of audit recommendations communicated to management. The auditor should document the rationale in deciding which audit recommendations should be followed up on and when, in contrast with recommendations where no follow-up is needed. The auditor should also follow up with management to document either that audit recommendations have been effectively implemented, or that senior management has accepted the risk of not implementing the recommendations. To the extent agreed upon with management, the internal audit unit should also monitor the disposition of recommendations arising for any non-audit services.

Maintaining Audit Documentation

Internal audit units should maintain documentation for each audit and subsequent follow-up. This documentation should contain sufficient information to enable an experienced auditor who has no previous connection with the audit to ascertain the evidence that supports the auditors’ significant judgments and conclusions. Each internal audit unit should establish a formal policy that clearly delineates who is responsible for reviewing audit documentation prepared by various staff levels and when that review should occur.

Audit documentation is the auditors' property and should be kept under their control. The auditors should know exactly where all pieces of documentation are at all times during the conduct of the audit. Approval from senior management and/or legal counsel should be obtained prior to releasing copies of audit documentation and reports to external parties. When not in use, documentation should be kept in a locked file or otherwise secured so as not to be readily available to persons who are not unauthorized to access it. This includes protecting electronic information with appropriate IT security controls. Audit documentation should be retained for a minimum of seven years after the date of the audit report. For recurring audits, the documentation supporting previous audits may be filed in a centralized record retention facility provided an individual is assigned to maintain a record of the location of each item sent to record storage and an appropriate destruction date is scheduled for the material.

External Quality Assessment Review

Professional audit standards require each internal audit organization to periodically undergo an independent review of the quality of its audit activities. The purpose of this review is to ensure that the organization’s quality control system is suitably designed and consistently complied with to the extent necessary to reasonably ensure compliance with audit standards. External assessments also promote more effective and efficient internal auditing operations by identifying better practices and making recommendations intended to improve performance. Periodic quality assessments are also an important means of reinforcing management’s confidence in the work of the internal audit unit. As such, each internal audit unit in New York State government must have an appropriate external quality assessment review performed at least once during every five-year period.

Appendix: Internal Control Reference Sources

Appendix: Internal Control Reference Sources

New York State Internal Control Act
http://www.osc.state.ny.us/agencies/ictf/docs/Internal%20Control%20Act.pdf?cl=39&a=73

New York State Internal Control Task Force Report – September 2006
New York State Internal Control Act Implementation Guide: Strengthening Compliance with the Act and Standards
http://www.osc.state.ny.us/agencies/ictf/docs/implement_guide_20060907.pdf

Internal Control - Integrated Framework (COSO)
http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf

New York State Division of the Budget – Budget Policy & Reporting Manual – Item B-350
Governmental Internal Control and Internal Audit Requirements
http://www.budget.ny.gov/guide/bprm/b/b350.html

ISACA - Control Objectives for Information and Related Technology (COBIT)
http://www.isaca.org/COBIT

U.S. Government Accountability Office - Standards for Internal Control in the Federal Government
http://www.gao.gov/products/GAO-14-704G

U.S. Government Accountability Office - Internal Control Management and Evaluation Tool
http://www.gao.gov/new.items/d011008g.pdf

Guidance on Control - The Canadian Institute of Chartered Accountants (COCO)
http://www.cica.ca

Association of Government Accountants (AGA)
http://www.agacgfm.org

Institute of Internal Auditors (IIA)
http://www.theiia.org

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

New York State Office of Information Technology Services
http://www.its.ny.gov/

Office of Management and Budget - OMB A-123 Management Accountability and Control
http://www.whitehouse.gov/omb/circulars/a123/a123.html

Public Company Accounting Oversight Board (PCAOB)
http://www.pcaobus.org/

The National Institute for Standards and Technology (NIST) – Special Publications Library
http://csrc.nist.gov/publications/PubsSPs.html

New York State Guide to Financial Operation: Section XI.11.F - Contract Monitoring
http://www.osc.state.ny.us/agencies/guide/MyWebHelp/Content/XI/11/F.htm

New York State Guide to Financial Operation: Section XII.4.D - Certification of Internal Controls over the Payment Process
http://www.osc.state.ny.us/agencies/guide/MyWebHelp/Content/XII/4/D.htm

Organizations can contact the Office of the State Comptroller to request specialized training on Internal Controls at: Outreach@osc.state.ny.us.

Contact

Office of the New York State Comptroller
110 State Street, 15th Floor
Albany, New York 12236

(518) 474-4015

www.osc.state.ny.us

Prepared by the Division of State Government Accountability

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller