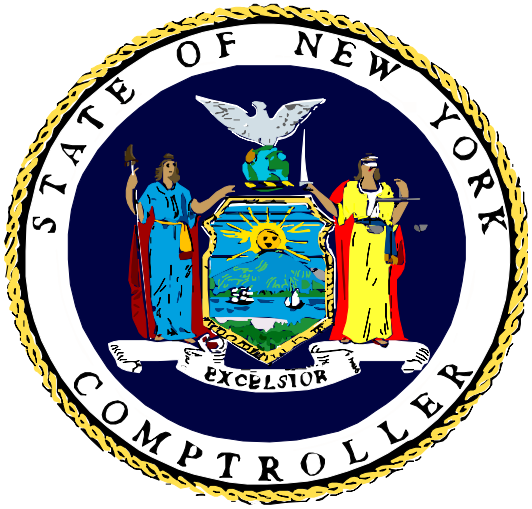
Standards for Internal Control

in New York State Government



October 2007

Thomas P. DiNapoli
State Comptroller

A MESSAGE FROM STATE COMPTROLLER THOMAS P. DINAPOLI

My Fellow Public Servants:

For over twenty 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. 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.

When these ***Standards*** were last revised in 2005, the New York State Internal Control Task Force was just being formed as a joint effort between my office, the Division of the Budget and the New York State Internal Control Association. In September 2006, the Task Force issued its report which recommended sweeping changes in the way the internal control and internal audit functions are managed, monitored and administered in New York State. While many recommendations require operating changes at the agency level, others call for clarification and greater specification in both the Budget regulations that govern the internal control program and these ***Standards*** against which the programs are measured. This revision incorporates 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.

Internal controls are much more than 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 receive the level 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.

Thomas P. DiNapoli
State Comptroller

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 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 have been compiled from those advocated by leading authorities in the field of internal control. All organizations subject to audit by the Office of the State Comptroller 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 the integration of the activities, plans, attitudes, policies, systems, resources and efforts of the people of an organization working together to provide reasonable assurance that the organization will achieve its objectives and 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 principles of internal control are rooted in well established organizational techniques and practices. These techniques and practices can best be understood as internal control if they are placed in the following conceptual framework: the five basic components of internal control (control environment, communication, assessing and managing risk, control activities, and monitoring) and the two supporting activities (evaluation and strategic planning). Accordingly, this publication is organized on the basis of this conceptual framework.

The application of internal control 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 web sites, 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 economy approximately the size of Canada. It is larger than most of the Fortune 500 companies. 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 people, 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 to our lives and our organizations. So, how can a subject of such importance be so unappreciated? The answer may lie in the need to better define internal control and what it does. This publication is intended to explain to New York State government employees how internal control plays an important part in their daily work activities.

Government managers should be able not only to account for funds spent on a program, but also to demonstrate the value of the program and 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. You should view them as the minimally acceptable standards for New York State government organizations.

These standards are not new ideas; many of the concepts are currently part of your existing operations. 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 professional organizations or 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 are similar 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. 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" goals and objectives are met, good internal control cannot guarantee organizational success. However, goals and objectives are much less likely to be met if internal control is poor.

Internal control is defined as follows:

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

This definition establishes that internal control:

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

FOUR PURPOSES OF INTERNAL CONTROL

While the overall purpose of internal control is to help an organization achieve its mission, internal control also helps an organization to:

1. Promote orderly, economical, efficient and effective operations, and produce quality products and services consistent with the organization's mission.

2. Safeguard resources against loss due to waste, abuse, mismanagement, errors and fraud.

3. Promote adherence to laws, regulations, contracts and management directives.

4. Develop and maintain reliable financial and management data, and accurately present that data in timely reports.

ORGANIZATIONAL ROLES

Every member of an organization has a role in the system of internal control. Internal control is people-dependent. It is developed by people; it guides people; it provides people with a means of accountability; and people carry it out. 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 attitude 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 the individuals performing the work have the skills and capacity to do so, and, to provide employees with appropriate supervision, monitoring, and training to reasonably assure 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. 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. While the internal control officer has responsibility for both implementing and reviewing the organization's internal control efforts, 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; the effectiveness of these procedures and requirements must be audited by someone who was not involved in the process of putting them into place. In contrast, the organization's internal auditor is responsible for evaluating the effectiveness of the system of internal control. This individual must be independent of the activities that are audited. For this reason, in most instances, the internal auditor cannot properly perform the role of internal control officer.

PART II: FIVE COMPONENTS OF INTERNAL CONTROL

CONTROL ENVIRONMENT

Control environment is the attitude toward internal control and control consciousness established and maintained by the management and employees of an organization. It is a product of management's governance, that is, its philosophy, style and supportive attitude, as well as the competence, ethical values, integrity and morale of the people of the organization. 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 describes how management is responsible for creating a positive control environment, and how employees are responsible for helping to maintain this environment.

Governance is the influence on an organization exercised by the executive body or the chief executive which/who governs it. 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/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/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 decisions and actions of senior managers;
- establishing high-level policy and organization structure;

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

Ethical Values and Integrity are key elements contributing to a good control environment. Ethical values are the standards of behavior that form the framework for employee conduct. Ethical values guide employees when they make decisions. Management addresses the issue of ethical values when it encourages:

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

People in an organization have personal and professional integrity when they adhere to ethical values. While it is management's responsibility to establish and communicate the ethical values of the 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.

Management 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 none are inherently right or wrong, 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 they reflect the ethical values of the organization, and positively affect 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: management's approach to recognizing and responding to risks (both internal and external); acceptance of regulatory control imposed by others; management's attitude toward internal and external reporting; the use of aggressive or conservative accounting principles; the attitude of management toward information technology and accounting functions; and management's support for and responsiveness to internal and external audits and evaluations.

Competence is a characteristic of people who have the skill, knowledge and ability to perform 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; and
- establishing training programs that help employees increase their knowledge and skills.

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

Morale is the attitude people have about their work, as exhibited by their confidence, discipline and willingness to perform tasks. Management should recognize the importance of good morale in an effective control environment. People's attitude about their jobs, work environment and organization affects how well they do their jobs. 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; and
- the lines of communication are open.

Supportive Attitude 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 that 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;
- 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 it.

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. During periods of change, it provides cohesion to the organization and helps keep it on its proper course. Without a clearly defined and communicated mission, an organization may drift aimlessly and accomplish little.

The mission of an organization should be a 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 it.

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

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

An organization 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 activities.

COMMUNICATION

Communication is the exchange of useful information between and among people and organizations to support decisions and coordinate activities. 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. Communication with customers, suppliers, regulators and other outside parties is also essential to effective internal control.

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 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 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;
- convey top management's message that internal control responsibilities are important and should be taken seriously; and
- convey and enable communication with external parties.

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

ASSESSING AND MANAGING RISK

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

Preparing to Assess Risk

Management should first ensure that it has identified all the operational and control objectives throughout the organization. Control objectives are generally derived from the four purposes of internal control (as defined in Part I) and are stated in terms that reflect the responsibilities of the

organization's sub-units. For example, the following two control objectives are derived from the first two purposes of internal control:

- *Ensure all applications are processed accurately* (from the first purpose of internal control: to promote orderly, economical, efficient and effective operations, and produce quality products and services consistent with the organization's mission).

- *Ensure access to electronic files is restricted to authorized personnel* (from the second purpose of internal control: to safeguard resources against loss due to waste, abuse, mismanagement, errors and fraud).

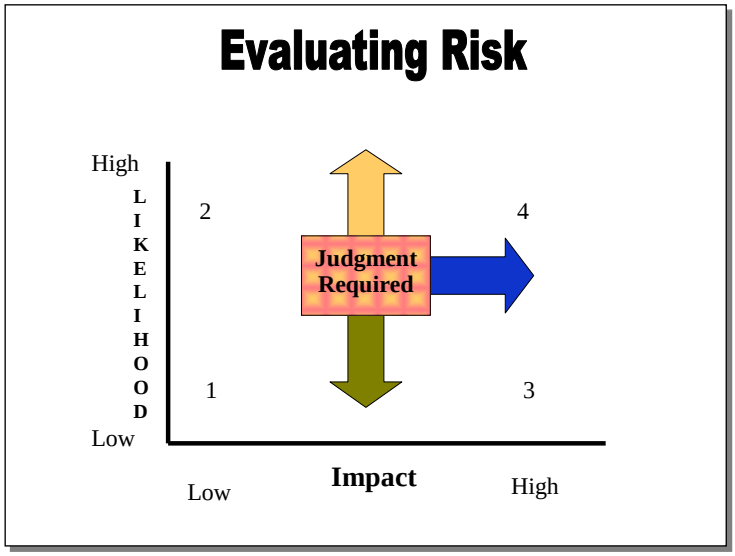
After identifying all the operational and control objectives, managers should identify all the risks associated with each objective (i.e., the events that would threaten the accomplishment of each objective). These risks can be both internal (e.g., human error, fraud, system breakdowns) and external (e.g., changes in legislation, natural disasters). It is essential that managers within the organization identify the risks associated with their respective objectives.

Risk Assessment Process

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 if the event were to occur. This effect could be some type of harm or an opportunity that would be lost. If possible, this effect should be quantified. At the very least, this effect 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 above chart graphically depicts a reasonable approach to evaluating risks, with quadrant 1 representing the lowest priority and quadrant 4 representing the highest priority risk. Management should use judgment to establish priorities for risks based on their impact and their likelihood of occurrence. Risks should be ranked in a logical manner, from the most significant (high impact) and most likely to occur (high likelihood) - as indicated in quadrant 4 - to the least significant (low impact) and least likely to occur (low likelihood), as indicated in quadrant 1 of the graph.

For example, a program manager has two cash accounts. One is the office petty cash fund and the other is for fees and fines from a program activity. Most people would consider the petty cash to

be a quadrant 1 or 2 assessment. When you discover the fees and fines, which are substantial in amount, are stored in an open location and there is a six-month backlog in processing them, this would be a quadrant 4 assessment. Your job is to drive down the level of risk from quadrant 4 to a lower level.

Management should use the information obtained from this assessment to help determine:

- how to manage risk;
- how to prevent or reduce risk; and
- how to manage risk during change.

Managing Risk

Executive management should provide guidance to managers throughout the organization to help them assess the level and the kinds of risk that are acceptable and not acceptable. Using this guidance and the risk assessment information, managers should determine whether to accept the risk in a given situation, prevent or reduce the risk, or avoid the 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 can accept the risk of unauthorized access because the consequences of such access are not significant; for example, the files may contain data that is not 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.

- *Prevent or 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 prevent the risk of unauthorized access, or at least reduce the risk to an acceptable level. However, the risk is prevented or reduced only as long as the control activities function as intended.

- *Avoid the risk: Do not carry out the function* - Management determines that it cannot tolerate any risk of unauthorized access to the files or that it 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).

Preventing or Reducing Risk

When preventing risk or reducing it to an acceptable level, management should 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?* Management should consider the reason the risk exists to help identify all the possible control activities that could prevent or reduce the risk.
- *What is the cost of control vs. the cost of the unfavorable event?* Management should compare the cost of the risk's effect with the cost of carrying out various control activities, and select the most cost-effective choice.
- *What is the priority of this risk?* Management should 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 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, preventing and reducing risk.

Managing Risk During Change

When change occurs in an organization (e.g., new processes, new systems, significant changes in job responsibilities, reorganizations, significant changes in personnel), it often affects the control activities that were designed to prevent or reduce risk. In order to properly manage risk, management should monitor any change to ensure that each risk continues to be managed as change occurs. Management should inform employees responsible for managing the organization's most critical risks about any proposed changes that may affect their ability to manage those risks. Managers should continually monitor the factors that can affect the risks they have already identified as well as other factors that could create new risks.

CONTROL ACTIVITIES

Control activities are tools - both manual and automated - that help identify, prevent or reduce the risks that can impede accomplishment of the organization's objectives. Management should establish control activities that are effective and efficient.

When designing and implementing control activities, management should try to get 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 significance and likelihood of the risk they are preventing or reducing.

Many different control activities can be used to counter the risks that threaten an organization's success. Most control activities, however, can be grouped into two categories: prevention and detection control activities.

- Prevention activities are designed to deter the occurrence of an undesirable event. The development of these controls involves predicting potential problems before they occur and implementing ways to avoid them.
- Detection activities are designed to identify undesirable events that do occur, and alert management about what has happened. This enables management to take corrective action promptly.

Prevention controls tend to be more expensive than detection controls. Costs and benefits should be assessed before control activities are implemented. Management should also remember that an excessive use of prevention 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. 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 and help form the basis for decisions made every day by employees. Without this framework of understanding by employees, conflict can occur, poor decisions can be made and serious harm can be done 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 flowcharts 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/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/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 sub-units 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 recordkeeping) should be done by different employees or sub-units 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;
- back-up and restore features of software applications that reduce the risk of lost data;
- virus protection software; and
- passwords that restrict user access to networks, data and applications.

IT control activities can be categorized as either general or application controls. General controls apply to all computerized information systems - mainframe, minicomputer, network and end-user environments. Application controls apply to the processing of data within the application software.

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. Organizations should have a plan that clearly describes the organization's security management program and policies and the procedures that support it, including procedures for the secure storage and disposal of sensitive information. Organizations should also establish a structure to implement and manage the security program with security responsibilities clearly defined. In addition, organizations 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 or 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; frequent changes of passwords and deactivation of former employees' passwords; frequent changes of dial-up numbers; and use of dial-back access.

- 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 sub-units 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 reestablishing 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 State Office of Cyber Security & Critical Infrastructure Coordination and by the New York State Office for Technology. Further guidance can also be obtained from sources such as the Information Systems Audit and Control Foundation's *Control Objectives for Information and Related Technology* and the Federal Government's National Institute for Standards and Technology's Special Publications.

MONITORING

Monitoring is the review of an organization's activities and transactions to assess the quality of performance over time and to determine whether controls are effective. Management should focus monitoring efforts on internal control and achievement of the organization's mission. For monitoring to be most effective, all employees need to understand the organization's mission, objectives, risk tolerance levels and their own responsibilities.

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 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 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 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 extended 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 a change in risk.

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 achieving 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 styles and philosophies foster accomplishment of the organization's mission.

- **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.

PART III: SUPPORTING ACTIVITIES

Evaluation, strategic planning and internal audit are all 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.

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 system of internal control 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 doing periodic assessments of the organization's performance compared to established expectations or measurement standards.

Evaluation can be accomplished through self-assessment and independent review. Self-assessment should be the primary basis for evaluation. 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. 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 sub-units found on an organization chart (e.g., a bureau), 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.

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 a listing 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 people 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 sub-units with their operational plans and objectives. Management should compare 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.

STRATEGIC PLANNING

Strategic plans are the courses of action that will 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. Based on the direction provided by 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

Objectives are the organization's desired outcomes. They are a product of the planning process and are necessary for coordinating efforts within an organization. Without clearly defined objectives, employees could be working inefficiently, ineffectively and/ or in conflicting directions.

Objectives can be organizational or operational. Management derives organizational objectives from the mission and often develops them during the strategic planning process. They are long-range, broad statements, which define the desired outcomes of the organization as a whole. Good

organizational objectives can serve as starting points for more specific and detailed objectives within the sub-units (i.e., divisions, departments, bureaus and assessable units) of the organization. They also serve as standards for evaluating overall organizational performance.

Management derives operational objectives from the broad organizational objectives. Operational objectives are shorter-range, more specific and define the desired outcomes of each of the organization's sub-units. They should be structured in a hierarchy so that each sub-unit'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 grow, 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 entitled *Government Internal Control and Internal Audit Requirements*.

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 and avoid 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 corporate governance. These values provide a basis that executive managers, audit committees and third parties can rely upon when considering the internal auditor's findings and recommendations. To ensure independence and objectivity, the internal audit function should ideally be organized under the chief executive and report directly to any

audit committee, board of directors or other governing authority that may exist. As a practical matter, internal audit directors in State entities may report to the deputy head of their organizations, such as the executive deputy commissioner, provided that person does not have line management responsibilities.

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 and as such, 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.

As a practical matter, smaller agencies may not have sufficient resources to fully separate their internal audit, 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, there needs to be clear communication, as part of that process, that agency managers are 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 unanimity 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 internal control officer 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 to independence 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 major part in New York State due to the provisions of the 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, the internal audit units must devote resources to examining their organization's 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 should periodically develop a risk-based plan of audit engagements to determine the priorities for the internal audit activity. This audit plan should be primarily 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 discussed in these Standards: control environment, information and communication, assessing and managing risk, control activities and monitoring. Depending on the needs of the agency, the audit unit may need to expand the scope of their inquiry even further.

Senior management and governing board input (where applicable) should also be considered in 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 are all subject to 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 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 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 their 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.

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

Standards for Internal Control in New York State Government
http://www.osc.state.ny.us/audits/audits/controls/standards.htm

Internal Control - Integrated Framework (COSO)
http://www.coso.org/publications.htm

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

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

Government Accountability Office - Standards for Internal Control in the Federal Government
http://www.gao.gov/special.pubs/ai2131.pdf

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 Cyber Security & Critical Infrastructure Coordination
http://www.cscic.state.ny.us/security/relevantlaws.htm

New York State Office for Technology
http://www.oft.state.ny.us

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/

Special Publications - The National Institute for Standards and Technology (NIST)
http://nvl.nist.gov/