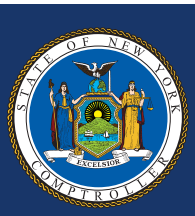


New York State Comptroller
THOMAS P. DiNAPOLI

Local Government Management Guide

Management's Responsibility for Internal Controls

January 2016

Table of Contents

Management's Responsibility for Internal Controls

Internal controls are essential to the effective operation of local governments and school districts. Simply put, internal controls are activities or procedures designed to provide reasonable assurance that operations are "going according to plan." Without adequate internal controls, management has little assurance that its goals and objectives will be achieved. Properly designed and functioning controls reduce the likelihood that significant errors or fraud will occur and remain undetected. Internal controls also help ensure that departments (other than the main finance office) are performing as expected.

When the subject of internal control is discussed, the conversation frequently centers on control activities or procedures, rather than the bigger picture of the whole internal control framework. To execute its responsibilities effectively, management needs to understand how an integrated internal control framework should work. This guide is designed to introduce local government and school managers and officials to the components of an integrated internal control framework.

This guide is designed to introduce local government and school managers and officials to the components of an integrated internal control framework.

The following topics are discussed in this guide:

- The Origin - Committee of Sponsoring Organizations (COSO)
- Integrated Internal Control Framework - The Big Picture
- The Five Essential Elements of Internal Control
- Limitations of Internal Controls
- The Impact of Information Technology
- The Role of Internal Auditors and Audit Committees.

Although this guide's focus is the theoretical concept of the integrated internal control framework, we have also published a companion guide, *The Practice of Internal Controls*, which contains guidance on practical control procedures that local governments and school districts can implement. For maximum understanding, these two guides should be read in conjunction with each other.

Who's Responsible?

The governing board's responsibilities for internal controls primarily involve oversight, authorization and ethical leadership.

This may come as a surprise to some readers, but external auditors are not responsible for an entity's internal controls. External auditors evaluate internal controls as part of their audit planning process, but they are not responsible for the design and effectiveness of your controls. As the title of this guide suggests, management (including the governing board) is responsible for making sure that the right controls are in place, and that they are performing as intended.

The governing board's responsibilities for internal controls primarily involve oversight, authorization and ethical leadership. Generally, governing boards do not design internal controls or prepare the written policies they adopt. The governing board relies upon management, especially the chief executive officer (CEO), to create the policies needed to ensure that services are provided effectively and assets safeguarded.[1] The CEO in turn relies upon managers and department heads to recommend and implement procedures that lower identified risks. Each board member should carefully review and seek to understand policies and procedures presented to them for ratification.

Within the managerial ranks, the CEO provides the leadership needed to establish and guide an integrated internal control framework. The CEO establishes a positive "tone at the top" by conducting an organization's affairs in an honest and ethical manner and establishing accountability at all levels of the organization. If the CEO does not demonstrate strong support for internal controls, the organization as a whole will be unlikely to practice good internal controls.

[1] Some examples of chief executive officers are: an appointed county manager or an elected county executive; an appointed town manager or an elected town supervisor; the mayor of a village or city; and the superintendent of a school district.

Finance officers (including school business officials) are instrumental in overseeing accounting and financial reporting controls. A finance officer's responsibilities for supervising the preparation of accounting records, producing financial reports and demonstrating compliance with State and federal laws are priority goals for local governments and school districts. Because of their vital responsibilities, finance officers should be knowledgeable about both control procedures and the integrated internal control framework taken as a whole. Finance officers and business officials also need to work closely with the CEO in fostering a positive control environment.

Even though the CEO leads the entity's approach to the control framework, it is the operational managers and department heads who are the front line for implementing and monitoring internal controls. 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 affect the controls they have put into place. Operational managers, however, rely upon the CEO to provide the leadership and the entity-wide communication needed to foster an integrated internal control framework.

The governing board, like the CEO, shapes the organization's tone-at-the-top by demonstrating integrity, honesty and ethical behavior in its handling of decisions and sensitive issues. Finance officers and operational managers support the internal control initiatives of the CEO and the governing board 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 meetings its goals and objectives.

Even though the CEO leads the entity's approach to the control framework, it is the operational managers and department heads who are the front line for implementing and monitoring internal controls.

The Origin - Committee of Sponsoring Organizations

The COSO model is widely recognized as the industry standard against which organizations measure the effectiveness of their systems of internal control.

The Committee of Sponsoring Organizations (COSO) of the Treadway Commission is a voluntary, private-sector initiative dedicated to improving the quality of financial reporting through ethics, effective internal controls and corporate governance. COSO is sponsored and funded by five major professional accounting associations and institutes.[2]

In 1992, COSO issued a report entitled *Internal Control - Integrated Framework*, which defined and changed the way internal controls were viewed.[3] The COSO framework considers not only the evaluation of hard controls, such as segregation of duties, but also soft controls, such as the competence and professionalism of employees. The COSO report presented a common definition of internal control and identified five key elements of a successful internal control framework. The COSO model is widely recognized as the industry standard against which organizations measure the effectiveness of their systems of internal control. The COSO framework also established the criteria used by government and other external auditors to assess the effectiveness of internal controls established by local governments.

Key Point

The COSO report defined internal control as "a process, affected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations."

[2] The American Institute of Certified Public Accountants (AICPA), the American Accounting Association (AAA), Financial Executives International (FEI), the Institute of Internal Auditors (IIA) and the Institute of Management Accountants (IMA).

[3] The report was published with minor amendments in 1994.

Integrated Internal Control Framework - The Big Picture

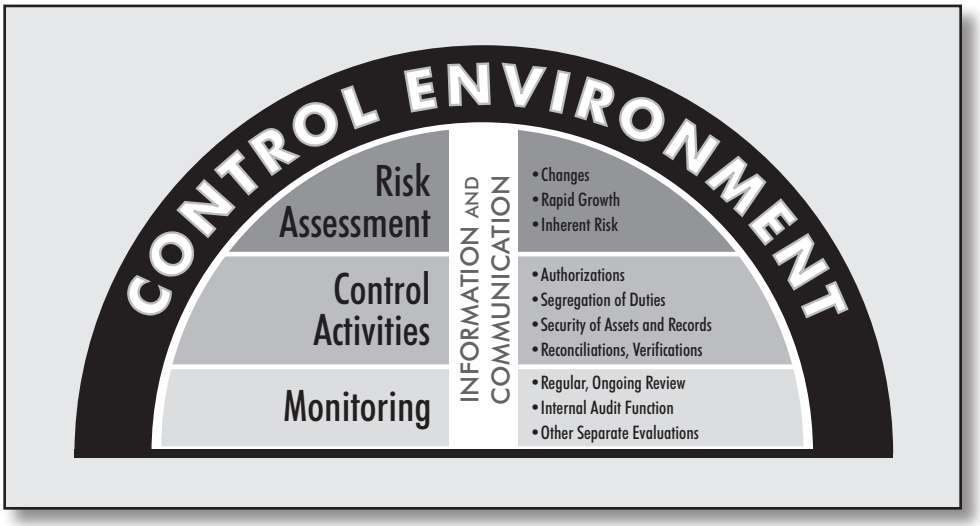
The five interrelated elements of an internal control framework, as identified by the COSO report, are:

- Fostering a favorable *control environment*
- Conducting *risk assessment*
- Designing and implementing *control activities* in the form of policies and procedures
- Providing for effective *communication* throughout the organization
- Conducting ongoing *monitoring* of the effectiveness of control-related policies and procedures.

The overall success of a system of internal controls is dependent on how effectively each of these elements functions and how well they are coordinated and integrated with each other.

The control environment is pervasive, as it affects (either positively or negatively) the entire organization and all other elements in the framework. It is the medium that spreads the organization's commitment to ethical and honest behavior, effective internal controls and proper financial reporting. Information and communication is another element that flows through the entire internal control framework. Information is the vehicle by which control policies and procedures are introduced and reinforced and communication is the conduit by which employees become aware of management's commitment to internal controls. Both the control environment and information and communication connect all elements of the framework together. The other fundamental elements of risk assessment, control procedures and monitoring are the building blocks that create, implement and review the policies and procedures that constitute a system of internal controls.

Information is the vehicle by which control policies and procedures are introduced and reinforced and communication is the conduit by which employees become aware of management's commitment to internal controls.



The Five Essential Elements of the Internal Control Framework

The governing board, chief executive officer and the entire management team all contribute to creating a positive control environment or "tone at the top."

Control Environment

The concept of the control environment can be difficult to understand, because the control environment is not something you can see or touch. You won't find the control environment embedded in a general ledger, or in any group of transactions or in any financial report. However, when the control environment is good (or poor), every employee will know it. Auditors are trained in assessing the control environment because it is a high-level indicator of how seriously management takes its responsibility for internal controls and how well management is meeting this responsibility. It is a highly subjective component of the internal control framework, but one well worth understanding.

In contrast to specific control procedures (like checking the mathematical accuracy of vendor invoices) which focus on a single processing stream, the control environment has a *pervasive* influence that affects all business decisions and activities of the organization. The governing board, chief executive officer and the entire management team all contribute to creating a positive control environment or "tone at the top." The governing board sets the proper tone for the control environment when it establishes and communicates a code of ethics, requires ethical and honest behavior from all employees, observes the same rules it expects others to follow, and requires appropriate conduct from everyone in the organization.

Additional factors that influence an entity's control environment are: management's philosophy and operating style; the way in which management assigns authority and responsibility; the way management organizes and develops employees; and the attention and direction provided by the governing board. The control environment sets the tone of the organization, influencing the control consciousness of all its employees.

Key Point

Creating the proper control environment for a local government is crucial to the effective implementation of all the other elements of the integrated framework. Staff members will take their cue from the attitude and example displayed by management. If employees see officials or department heads abusing their authority or not being held accountable to appropriate policies, then employees may also begin abusing those policies. As the old saying goes, "Actions speak louder than words." Management must communicate its support for internal controls to all levels of staff within the organization. The control environment is enhanced by written policies governing employee activities that are communicated to employees to act upon.

Factors Affecting Risk Assessment

The design of internal controls to fit an organization's needs begins with a risk assessment process. Risk assessment is the identification of factors or conditions that threaten the achievement of an organization's objectives and goals. It involves identifying risks to the effectiveness and efficiency of financial and service operations, to the reliability of financial reporting, and to compliance with laws and regulations. Every local government and school district needs to conduct an assessment to identify risks to its operations. Before that assessment begins, managers need to understand and consider several qualitative factors that can affect their assessment.

Risk assessment is the identification of factors or conditions that threaten the achievement of an organization's objectives and goals.

Inherent Risk

The nature and characteristics of certain activities and assets puts them at greater risk for fraud or material error. This condition is referred to as inherent risk. Some characteristics that generally increase inherent risk are:

- **Opportunity** - The more liquid or mobile an asset is, or the more decentralized an operation is, the greater the potential for fraudulent activity. For example, inherently risky assets include laptop computers and other portable electronic equipment, cash (especially undeposited cash) and gasoline. Inherently risky operations include the collection of cash in almost any venue, loaning and storage of electronic equipment, and credit card and cell phone usage.

- **Unfamiliarity** - The newer the activity or program, the greater the possibility that its operation and risks may not be well understood and its objectives and goals may not be realized. New services may require unique internal control policies and procedures, or may require modification of existing internal controls. For example, when a new recreational facility is opened, procedures for the collection and deposit of fees may not be in place or be well understood by employees. On the operational side, liability insurance may not be adequate to indemnify the organization against claims that may occur because of citizen or spectator injuries.

- **Complexity** - The more complex an activity is, the greater the possibility of errors occurring. For example, legal and grant requirements governing aid programs may increase the likelihood that significant noncompliance and eligibility concerns may occur. When planning a large capital project, management may not be sufficiently familiar with the oversight, financial, legal and insurance requirements of construction projects, leading to unexpected costs and delays in completing the project.

Because conditions impacting operations will change continuously, your risk assessment needs to identify and analyze risks associated with such changes.

Management needs to identify and analyze inherently risky assets and operations early and frequently in the risk assessment process.

Change

Another factor impacting the risk assessment process is the element of change. Because conditions impacting operations will change continuously, your risk assessment needs to identify and analyze risks associated with such changes. Some examples of change that you should consider are:

- **Changes in Operating Environment** - Both internal change and external change impacts the environment in which employees work and may affect the entity's ability to achieve its objectives. Externally, new or revised regulations that affect a major program or an aid category can present both financial and service delivery risks. Internally, new or updated financial management software can create increased risk of accounting errors and untimely financial reports. Changes in information technology, both internal and external, can be particularly challenging because of the specialized expertise that may be required to design, implement and monitor information system controls.

- **Changes in Personnel** - Staff turnover can impact the achievement of the entity's objectives because it takes time for new employees to achieve the proficiency of the employees they are replacing. Frequent staff turnover, especially in the same position, may be indicative of other symptoms that are worthy of risk assessment as well. Changes in personnel may compromise the functioning of specific internal controls or, in the case of certain management positions, the functioning of the entire control framework. New personnel should be trained about internal control policies and procedures and understand their specific responsibilities.

Managers need to anticipate significant changes within the organization and in their areas of responsibility as early as possible, analyze how risks will be affected by these changes and determine whether the design of existing controls will be adequate.

Rapid Growth

Rapid increases in the number of residents living in an area or school district, retail expansion or other forms of economic stimulus can mean greater demands for public services. Such demands can impact the ability of a department, local government or school district to provide adequate levels of service in a cost-effective manner. The increase in demand may even necessitate re-evaluating the entity's objectives. Any time there is increased demand for public services, the adequacy of existing efficiency controls should also be examined.

The Process of Risk Assessment

The purpose of risk assessment is to identify those events, conditions or risks that could significantly affect the achievement of the organization's objectives, including the protection of assets and the efficient operation of financial operations and other services. Risk assessment can begin by asking a series of predetermined questions, obtaining answers and analyzing the results. Except for school districts, there is no required time frame for conducting a risk assessment.[4] A prudent approach would be to conduct an entity-wide risk assessment at least annually.

Some questions that could be asked in an entity-wide risk assessment are:

What are our primary objectives?

- What must go right for us to succeed?
- What events or conditions can prevent us from achieving these objectives?
- Which of our assets are most liquid or desirable and, therefore, in most need of protection?
- What information do we rely on to achieve our objectives? What are the threats to our obtaining this information?
- What typical decisions are made in our operations? Which of these decisions require the most judgments?
- What are our most complex activities?
- What potential legal liabilities can result from our operations?
- Where do we spend most of our money?
- What changes do we see on the horizon?

Risk assessment should begin at the top of the organization and reach down in an organized fashion to the department level and to particular activities and processes within departments. Remember to focus your efforts on those risks that are significant to the achievement of the organization's financial and service objectives, and that have a reasonable likelihood of occurrence.

Risk assessment should begin at the top of the organization and reach down in an organized fashion to the department level and to particular activities and processes within departments.

[4] Education Law Section 2116-b requires most school districts to have an internal audit function that includes the development of a risk assessment of district operations, including but not limited to: a review of financial policies and procedures and the testing and evaluation of district internal controls; an annual review and update of such risk assessment; and preparation of reports, at least annually or more frequently as the trustees or board of education may direct.

It's always helpful to document the results of your risk assessment to facilitate further analysis and periodic updates. The previous or similar questions can be recorded in a table similar to the one below:

Objectives	Risks to Achieving Objectives	Controls in Place	Control Deficiencies	Corrective Action
Instructions: List the primary objectives of the entity, department, program or activity.	Risks should be associated with a listed objective. There are a multitude of risks that could be identified regarding each objective. Focus on significant risks with a reasonable likelihood of occurrence.	For each risk, identify controls that exist to prevent the risk from occurring and to help detect the occurrence of the risk.	Identify where the design of current controls may not be sufficient to mitigate risk, and where existing controls may not be operating effectively. Note: internal auditors and audit committees can be a valuable source of information about potential control deficiencies.	List the corrective action to be taken and who will be responsible for implementing the action.
Example: Bank deposits and investments are protected from loss.	During peak cash flow periods, bank deposits and investments exceed FDIC insurance.	A security and custodial agreement is in place.	The agreement has not been reviewed in several years, may not be current, and the level of pledged securities may no longer be adequate. Also, there is no agreement with a new depository where deposits also exceed FDIC insurance.	The chief fiscal officer or business manager will: 1) Compare bank deposits at peak periods to pledged collateral amounts. 2) Contact new depository to obtain security for deposits in excess of FDIC insurance. 3) Present all agreements to legal counsel to verify that agreements meet statutory requirements.

Control Activities

The third component of the integrated framework is control activities. Control activities are the policies and procedures designed by management to help ensure that the organization's objectives and goals are not negatively impacted by internal or external risks. Some common and important control procedures are bank reconciliations and the review of those reconciliations by supervisory personnel; segregation of duties so that no one person controls all phases of a transaction cycle; daily deposit of cash receipts; frequent password changes; and limiting access to check stock, signature plates and wire transfer software.[5] Control procedures can also be used to keep costs as low as possible. A common procurement control procedure is to require oral or written quotes for purchases not subject to competitive bidding. This procedure is used to lower the risk that cost conscious purchases will not be made.

Control activities are the policies and procedures designed by management to help ensure that the organization's objectives and goals are not negatively impacted by internal or external risks.

The COSO report identified a range of control activities including: approvals, authorizations, verifications, reconciliations, and reviews of operating performance, security of assets and segregation of duties. These and other control activities can be divided into four categories:

- **Directive controls** provide guidance to employees to help achieve the desired objectives of the department. For example, a job description would be a directive control that would provide employees with guidance as to what is expected of them. A personnel policy or code of ethics would provide guidance on the conduct expected of all employees.
- **Preventive controls** are designed to deter the occurrence of errors or other undesirable events. An example of a preventive control is segregation of duties. Segregation of duties is primarily designed to prevent fraudulent activity from occurring and remaining undetected by dividing key financial tasks among two or more people.
- **Detective controls** identify on a timely basis when errors or other undesirable events have occurred. Some examples of detective controls are reconciliations and reviews of performance. Examples of reconciliations are comparisons of cash amounts in the general ledger to cash balances in reconciled bank statements, and physical counts of fixed assets against amounts recorded on inventory records. Management can detect budgetary problems by comparing information about financial performance with budgets, prior periods, or other benchmarks to measure the extent to which financial goals and objectives are being met.

[5] For additional guidance on control procedures, see our Local Government Management Guide, *The Practice of Internal Controls*, available on our website at **http://www.osc.state.ny.us/localgov/pubs/lgmg/practiceinternalcontrols.pdf.**

In general, preventive controls are stronger than detective controls because they prevent mistakes and other undesirable events from occurring.

- **Corrective controls** identify the flaws in the process and determine the actions to be taken to correct the problems. Examples of corrective controls are additional employee training and reassessment of the current procedures.

In general, preventive controls are stronger than detective controls because they prevent mistakes and other undesirable events from occurring. Detective controls are important too, but they often detect mistakes or other events after they have occurred, making it more difficult to correct the mistake or recover from the undesirable event. For example, monitored access to a fuel pump is a preventive control. When this control operates properly, it should prevent inappropriate usage of fuel for personal or other unauthorized purposes. A periodic reconciliation of fuel usage is a detective control that should also be in place. However, if a mistake or theft of fuel does occur because the preventive control failed or was overridden, the fuel is already gone by the time that the reconciliation identifies the loss. Thus preventive controls are stronger controls for preventing errors and fraud from occurring.

Key Point

Control activities should be designed to limit the potential negative effects of risks identified during the assessment process. Some risks may be so remote or the effects of such risks so minor that you may decide simply to accept those risks without developing controls to address them. Some risks, if they occur, may be so significant that, even though remote, they need to be limited. For these risks, management may decide to purchase insurance. For all other risks (and even for risks that are insured) managers should implement controls that will reduce the likelihood of such risks occurring or reduce the impact if such risks do occur.

Information and Communication

Information and Communication is the fourth essential element of the internal control framework. Like the control environment, information and communication has a global, interconnecting effect on the internal control framework. In order for risks to be controlled, it is imperative that there be a sound communication process that captures information and then provides information to all who have need of it. Since controlling risk is the responsibility of all managers and department heads, information about identified risks and the means of controlling those risks needs to be communicated to all who are responsible for mitigating those risks. Information about the policies and procedures to be followed by employees should flow down through the organization.

Since controlling risk is the responsibility of all managers and department heads, information about identified risks and the means of controlling those risks needs to be communicated to all who are responsible for mitigating those risks.

It is also important that the communication system allows for information to flow in all directions throughout the organization to lessen the chance of misunderstandings. Information about daily activities may flow across the organization from employees who develop the information to those who need the information. Problems may be identified at the lower levels of the organization (by rank-and-file employees); if the information is not allowed to flow back up to those who are responsible for making corrections, managers will not receive needed information on time.

The executive summary to COSO states, "Pertinent information must be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities. Information systems produce reports containing operational, financial and compliance-related information that make it possible to run and control the business." COSO also states that information must flow throughout the organization so that individuals understand their own roles in the internal control system and how their work relates to the work of others.

As part of the information and communication system, it is important to inform all employees that control responsibilities are to be taken seriously. Each employee should understand his or her role in the internal control system, as well as how their individual activities relate to the work of others. Employees also need to know that they have a responsibility to communicate problems they notice in the performance of their duties.

Monitoring determines whether or not policies and procedures designed and implemented by management are being conducted effectively by employees.

Monitoring

The fifth essential element of an integrated internal control framework is monitoring. Monitoring determines whether or not policies and procedures designed and implemented by management are being conducted effectively by employees. Monitoring also helps ensure that significant control deficiencies are identified timely and rectified. Over time, new risks may arise or internal or external changes may impact the risk exposure of local governments and school districts. Monitoring helps to identify these new risks and the need for new control procedures. For example, upgrading to a new financial management application may expose an organization to new risks related to the accuracy of accounting records, or may increase opportunities for fraud or abuse to occur and remain undetected. The responsibility for overseeing the monitoring function generally falls to the CEO and the chief fiscal officer or, in schools, to the business official. The CEO should communicate to all managers that monitoring is an essential element of the internal control framework and is necessary to ensure that identified risks are controlled.

Since most local governments do not have internal auditors, the monitoring of internal controls will generally be conducted by managers and supervisors with responsibilities for financial operations and other services. These managers and supervisors will need to understand the risks that exist in their areas of responsibility and the controls that have been put in place to mitigate these risks. For example, a health insurance administrator may have instituted a control to verify retirees' health insurance coverage. Once the control is put in place, the administrator should periodically review the results of inquiries or searches conducted to verify that retirees (or their dependants) are still eligible for health benefits. Paying for health insurance for deceased retirees is a hidden cost, not always detected, unless there is a control procedure in place to verify eligibility and need periodically. The monitoring function ensures that this type of control is applied at least annually, and that reasonable assurance is obtained that unnecessary costs are not being incurred.

Limitations of Internal Controls

Internal controls provide reasonable but not absolute assurance that the entity's goals and objectives will be achieved. Any system of internal controls has limitations. Some of the most common limitations are cost-benefit relationships, collusion and management override.

When designing the internal control framework and in particular, specific control procedures, it is important to compare the potential benefits to be achieved (in terms of lowering risk and achieving objectives) with the cost of implementing such controls. Some control procedures that provide the most assurance may be too costly to implement and other, less costly, compensating controls may have to be substituted. For example, in a small village or fire district where the treasurer is responsible for all financial operations, it may not be cost-effective to hire another employee for the sole purpose of segregating the treasurer's duties. Instead, a more cost-effective control is to have board member, for example, periodically review the work of the treasurer, especially monthly bank reconciliations, to compensate for the lack of segregation of duties. Small and medium-sized local governments and school districts may need to utilize this type of approach to ensure proper controls are in place and to avoid incurring additional costs.

When designing the internal control framework and in particular, specific control procedures, it is important to compare the potential benefits to be achieved (in terms of lowering risk and achieving objectives) with the cost of implementing such controls.

The governing board and the CEO should also be aware that collusion between two or more employees can defeat a system of controls. Simply put, collusion is a secret agreement or cooperation between two or more employees for an illegal or dishonest purpose. Often internal controls are designed so that one employee functions as a check on another employee's work. In such situations, there is always the risk that employees who are supposed to perform independent control procedures may instead choose to work together to circumvent management's controls. It is difficult to set up a system of internal controls to protect against collusion. Management needs to be alert to close personal and family relationships that might present opportunities to circumvent in place controls. This is especially true when a supervisor or manager is responsible for monitoring control procedures performed by a family member or close personal friend.

Finally, even though internal controls are well-designed and effective, the same controls may be overridden by management itself. Management's position in the organizational hierarchy creates an opportunity to manipulate or override otherwise effective and properly designed controls. Management generally has the authority to direct that controls be bypassed or ignored at any time. Internal auditors or confidential fraud/abuse hotlines can help to mitigate the possibility of management override for personal gain or other fraudulent purposes. The bottom line, however, is that hiring and promoting managers with good character and high ethical values can go a long way in building a positive control environment and diminishing the risk of management override of controls.

The Impact of Information Technology

Even if the chief financial officer or business official does not act as the system administrator, this manager should be knowledgeable in system administration and be able to verify that appropriate levels of access are being maintained.

In addition to the traditional hard and soft controls already discussed, the CEO and other managers need to be cognizant of the impact of information technology (IT) on the integrated internal control framework. Gone are the days when government and school district financial management systems were based on manual processes. Even in the smallest of local governments, it's rare to find an accounting system (including general ledger and other systems) that is not fully or at least partially computerized. Manual financial systems are virtually nonexistent in the school district community.

What all of this means is that the governing board, CEO and other managers need to be aware that there are formidable risks connected with digital environments. What makes these environments so challenging is that the processing of financial transactions and the storage of sensitive information is virtually unseen and unheard, and modifications and intrusions into these systems are equally silent. The opportunities for the manipulation of data are high, especially if a dishonest and unethical individual is more knowledgeable in the functioning of the software than management is. Probably the single most important and easiest control to implement is limiting access to the system administration sector of the entity's financial management software. This sector grants access rights to the different modules included in the software (for example, payroll, accounts payable, general ledger) and also allows the system administrator to set up and modify certain application controls. As a general rule of thumb, system administrator status should be granted to a limited number of trusted employees. Even if the chief financial officer or business official does not act as the system administrator, this manager should be knowledgeable in system administration and be able to verify that appropriate levels of access are being maintained. Just like the concept of division of duties is applied in a manual environment, employees should only be granted access to those accounting modules that they need to perform their work. A second universally important IT control is the availability and periodic review of audit logs. An audit log records changes made in the administration of the financial management system, and also records any events where previously recorded (original) data is modified or system parameters are changed, even if temporarily. Audit logs can be an important detection control for possible manipulation of the financial data or other sensitive information.

The bottom line is that most CEOs and financial managers will need the help of a qualified IT professional to adequately assess the risks, design and monitor controls in a digital environment. Properly trained and knowledgeable internal auditors may be able to assist in reducing the risks associated with computer processed data and transactions.

The Role of Internal Auditors and Audit Committees

Internal auditors and audit committees enhance the effectiveness of the control framework and assist the governing board in meeting its oversight responsibilities for internal controls. Although these groups report to the governing board, they may in the course of their responsibilities collaborate with management in assessing risk, designing and monitoring controls. Internal auditors and audit committees have separate and distinct objectives and responsibilities.

Internal auditors and audit committees enhance the effectiveness of the control framework and assist the governing board in meeting its oversight responsibilities for internal controls.

Internal Auditor

The role of the internal auditor is that of an objective advisor with respect to the design and effectiveness of internal controls implemented by management. The internal auditor examines and reports to the governing board about the design and effectiveness of internal controls. The internal auditor will test how well existing internal controls are functioning, and recommend necessary changes and improvements. Ideally the internal auditor will work closely, but independently, with management and the audit committee (if one exists) to strengthen the system of internal controls and adapt it to new risks and changing conditions.

The internal auditor should report directly to the governing board or, if the board has established an audit committee, then to that committee. The more independent the internal auditor is from management, the more likely his or her work is to serve the organization's needs. Broadly speaking, the internal auditor supplements management oversight by independently monitoring whether adopted policies and procedures are being followed. The internal auditor's work should focus on areas with the greatest inherent risk of error or fraud. Internal audit functions include:

- Performing examinations of operating and financial controls
- Conducting efficiency and effectiveness reviews
- Conducting reviews of compliance with laws and other external regulations
- Evaluating the design and execution of internal controls.

[T]he establishment of the internal audit function provides another approach for monitoring the effectiveness of internal controls.

All but the smallest school districts are required by Education Law to establish an internal audit function.[6] Whether conducted by an in-house internal auditor or by an external auditor engaged for the purpose of internal auditing, the establishment of the internal audit function provides another approach for monitoring the effectiveness of internal controls.

Larger units of local government (or several smaller local governments acting together) can establish an internal audit function to monitor the effectiveness of their internal controls. Like school districts, local governments can establish an in-house internal audit function or they can obtain internal audit services via contract from a qualified, external professional or firm. In the absence of an internal audit function, the responsibility for monitoring internal controls lies solely with management.

[6] See section 2116-b (2) of Education Law.

Audit Committee

More commonly found in the corporate environment, audit committees are also being established in school districts, and to a lesser extent in local governments. Generally, the role of the audit committee is to help the governing board understand and collaborate with the annual (external) audit process. The traditional responsibilities of the audit committee are: to review and discuss with the external auditor the risk assessment developed as part of its audit planning process; to receive and review the draft audit report and management letter; to assist the board in interpreting these documents; and to make a recommendation to the board regarding the acceptance of the annual audit report.

In similar fashion, the audit committee can act as a liaison between the internal auditor and the board. Possible additional roles for the audit committee include:

- Making recommendations to the board regarding the appointment of the internal auditor.
- Assisting in the oversight of the internal audit function, including reviewing the annual internal audit plan to ensure that high risk areas and key control activities are periodically evaluated and tested.
- Reviewing the results of internal audit activities.
- Monitoring implementation of the internal auditor's recommendations.
- Participating in the evaluation of the performance of the internal audit function.

All but the smallest school districts are required by Education Law to establish an audit committee to assist the school board with its financial oversight responsibilities.[7] This committee may be made up of all or some of the members of the board of education, but it also can be made up in part or completely of people who are not board members. The guiding principle is that this committee should be able to help the board select and oversee external and internal auditors, exercise its financial oversight responsibility, and implement any necessary corrective reform. Even though the requirement for an audit committee pertains only to school districts, local governments may utilize this approach also.

All but the smallest school districts are required by Education Law to establish an audit committee to assist the school board with its financial oversight responsibilities.

[7] See section 2216-c of Education Law.

Conclusion

We have emphasized that internal controls have limitations, and managers need to know that even the best system will only provide reasonable (not absolute) assurance that financial reporting errors, fraud and operating inefficiencies will be identified and controlled.

If this guide teaches you anything, we hope it has taught you this: *As a local government or school district board member, CEO or manager, your responsibility for overseeing internal controls isn't a once-a-year task*. Just like many of the other activities you manage, overseeing the framework of internal controls commands your attention throughout the year, not just when the auditors arrive. To do a good job of having the right controls in place, you need to build risk assessment and monitoring into your weekly and monthly management processes. School districts are required by statute to perform an annual risk assessment, and many districts have hired professional auditors to meet this requirement. An annual evaluation, although helpful, shouldn't be the only time that risk assessment and monitoring occurs. Every CEO and every manager should be alert for new and changing risks at all times. Communicating these new risks to those charged with performing your risk assessment is very helpful, but management needs to be able and willing to design or modify controls as soon as new risks are identified.

We have emphasized that internal controls have limitations, and managers need to know that even the best system will only provide reasonable (not absolute) assurance that financial reporting errors, fraud and operating inefficiencies will be identified and controlled. The level of assurance that your system provides may very well be determined by the amount of monitoring conducted by management. When management takes the time to find out if controls are being implemented as designed, a message is sent to all employees that internal controls are important. Conversely, when management doesn't pay attention to controls that they think are in place, it is probable that these controls are not functioning effectively. In addition to performing some level of continuous monitoring, management needs to communicate its expectations for internal controls to all employees, and to establish a system of communication that relays information from the bottom of the organization to the top and vice versa. The tone at the top regarding internal controls will determine to a great extent the success of the various elements of the internal control framework.

We would be pleased to assist you with any questions you have regarding the information contained in this guide. The addresses and telephone numbers for each of our regional offices and our legal staff are located at the end of this publication.

Additional Resources

New York State has utilized the COSO Integrated Framework in developing its approach to controlling risks at the agency level. Information on New York State's approach to internal controls can be found at the following web addresses:

Office of the State Comptroller - Internal Control Task Force

http://www.osc.state.ny.us/agencies/ictf

Standards for Internal Control in New York State Government

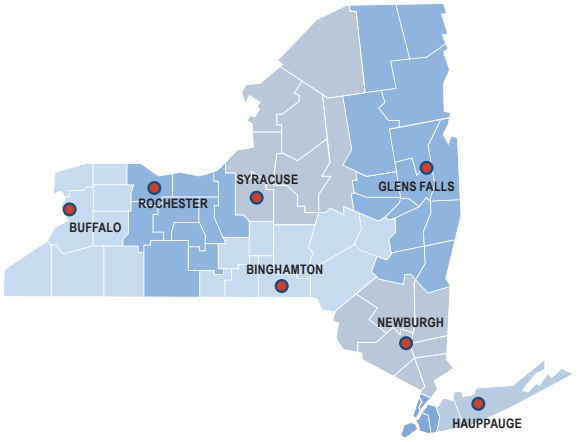
http://www.osc.state.ny.us/agencies/ictf/docs/intcontrol_stds.pdf

New York State Comptroller
THOMAS P. DiNAPOLI

Division of Local Government and School Accountability

110 State Street, 12th Floor, Albany, NY 12236
Tel: 518.474.4037 • Fax: 518.486.6479
Email: localgov@osc.ny.gov

www.osc.ny.gov/local-government



Andrea C. Miller
Executive Deputy Comptroller

Executive • 518.474.4037
Robin L. Lois, CPA, Deputy Comptroller
Simonia Brown, Assistant Comptroller
Randy Partridge, Assistant Comptroller

Audits, Local Government Services and Professional Standards • 518.474.5404
(Audits, Technical Assistance, Accounting and Audit Standards)

Local Government and School Accountability Help Line • 866.321.8503 or 518.408.4934
(Electronic Filing, Financial Reporting, Justice Courts, Training)

Division of Legal Services
Municipal Law Section • 518.474.5586

New York State & Local Retirement System
Retirement Information Services
Inquiries on Employee Benefits and Programs
518.474.7736

Technical Assistance is available at any of our Regional Offices

BINGHAMTON REGIONAL OFFICE
Tel 607.721.8306 • **Fax** 607.721.8313 • **Email** Muni-Binghamton@osc.ny.gov
Counties: Broome, Chemung, Chenango, Cortland, Delaware, Otsego, Schoharie, Tioga, Tompkins

BUFFALO REGIONAL OFFICE
Tel 716.847.3647 • **Fax** 716.847.3643 • **Email** Muni-Buffalo@osc.ny.gov
Counties: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming

GLENS FALLS REGIONAL OFFICE
Tel 518.793.0057 • **Fax** 518.793.5797 • **Email** Muni-GlensFalls@osc.ny.gov
Counties: Albany, Clinton, Columbia, Essex, Franklin, Fulton, Greene, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington

HAUPPAUGE REGIONAL OFFICE
Tel 631.952.6534 • **Fax** 631.952.6530 • **Email** Muni-Hauppauge@osc.ny.gov
Counties: Nassau, Suffolk

NEWBURGH REGIONAL OFFICE
Tel 845.567.0858 • **Fax** 845.567.0080 • **Email** Muni-Newburgh@osc.ny.gov
Counties: Dutchess, Orange, Putnam, Rockland, Sullivan, Ulster, Westchester

ROCHESTER REGIONAL OFFICE
Tel 585.454.2460 • **Fax** 585.454.3545 • **Email** Muni-Rochester@osc.ny.gov
Counties: Cayuga, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates

SYRACUSE REGIONAL OFFICE
Tel 315.428.4192 • **Fax** 315.426.2119 • **Email** Muni-Syracuse@osc.ny.gov
Counties: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence

STATEWIDE AUDIT
Tel 607.721.8306 • **Fax** 607.721.8313 • **Email** Muni-Statewide@osc.ny.gov

osc.ny.gov

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability

110 State Street, 12th floor
Albany, NY 12236
Tel: (518) 474-4037
Fax: (518) 486-6479
or email us: localgov@osc.ny.gov

www.osc.ny.gov/local-government

Original Release October 2010

Updated January 2016