State of New Jersey

Office of the State Comptroller

INTERNAL CONTROL GUIDE

A. Matthew Boxer
State Comptroller

November 2011

Table of Contents

Part I

Part II

Part III

PART I

INTRODUCTION

Management of an organization involves four basic functions: planning, organizing, leading, and controlling. An internal control system should be an integral part of managing any organization. Such a system includes the plans, methods, and procedures used to meet the entity's goals and objectives. Effective management requires internal controls that allow managers to delegate responsibilities to staff and have comfort that their expectations will be realized.

This Internal Control Guide can be utilized by all New Jersey State departments, agencies, authorities, and units of local government regardless of size and structure to assist them in establishing and maintaining an effective internal control system. Its purpose is to provide general information regarding the essential elements necessary for an effective internal control system, a brief overview of different types of fraud and information concerning other resources and reference materials.

This guide is based mainly on the standards contained in the 1992 Committee of Sponsoring Organizations (COSO) report, *Internal Control - Integrated Framework*. That report details the basic standards of internal control that can be used by all organizations. This Internal Control Guide is being made available to all state and local government employees to assist them in understanding the COSO standards of internal control and to assist management with establishing the framework for developing, implementing and monitoring their own internal control systems.

This guide is not all-inclusive. Nor is it intended to set forth the exact steps to be taken by an entity. It's goal is to provide guidance that will assist the entity in the development and implementation of an internal control system that meets their specific needs. Entity-specific considerations must be evaluated in the development and implementation of appropriate and effective internal controls. Continuous review and monitoring is also necessary to ensure that the controls in place meet the needs of the entity and are working as intended.

Suggestions and comments regarding this guide can be directed to the Office of the State Comptroller at www.state.nj.us/comptroller/ or at 609-984-2888.

COSO AND THE INTERNAL CONTROL FRAMEWORK

COSO is a private-sector organization dedicated to guiding executive management and governance entities toward the establishment of more effective, efficient, and ethical business operations. It sponsors and disseminates frameworks and guidance based on in-depth research, analysis, and best practices.

History

COSO was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting (Commission), an independent private-sector initiative which studied the causal factors that can lead to fraudulent financial reporting. The Commission also developed recommendations for public companies and their independent auditors, for the Securities and Exchange Commission (SEC) and other regulators, and for educational institutions.

In 1992, COSO issued the Internal Control – Integrated Framework report. The internal control framework and principles noted in that guide are generally recognized in the United States as the model for internal control.

The basic principles provide that internal control is comprised of a number of interrelated components that work together to achieve an organization's goals. They are derived from the way management runs an organization and are integrated with the management process. These components apply to all organizations but smaller organizations may implement them differently than larger ones – they may be less formal or less structured.

These components define the standards for internal control and provide the basis against which internal control is to be evaluated.

In 2004, COSO was updated to incorporate within it an Enterprise Risk Management (ERM) framework. ERM embodies the methods and processes used by organizations to identify potential events that may affect the entity, to minimize related risks so they are within acceptable limits, and to provide reasonable assurance regarding achievement of the entity's objectives. For further information on ERM see http://www.coso.org/documents/COSO_ERM_ExecutivesSummary.pdf .

PART II

UNDERSTANDING INTERNAL CONTROL - THE BASICS

What is Internal Control?

COSO defines internal control as:

> a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
>
> - effectiveness and efficiency of operations;
> - reliability of financial reporting; and
> - compliance with applicable laws and regulations.

An internal control system comprises the plans, methods, and procedures used to meet an organization's mission, goals and objectives. Internal control also serves as the first line of defense in safeguarding assets and preventing and detecting errors and fraud. It is designed to provide reasonable assurance that the objectives and mission of the organization are being achieved. Internal control also helps an organization to promote economical, efficient and effective operations; safeguard resources against loss; promote adherence to laws and regulations; and develop and maintain reliable financial and management data.

Fundamental Concepts of Internal Control

Internal control is a continuous built-in component of operations, effected by people and geared to the achievement of the entity's objectives. Internal control provides reasonable, but not absolute assurance that entity objectives will be met. Internal control helps to regulate and guide every aspect of the organization and its operations. As the organization evolves, the internal control system will change. The degree of control employed is a matter of business judgment. Generally, the cost of a control should not exceed the benefit to be derived from it. When business controls are found to contain weaknesses, consider the following alternatives:

- increase supervision and monitoring;
- institute additional or compensating controls; and/or
- accept the risk inherent with the control weakness (assumes management approval).

An effective internal control system enables the entity to manage significant risks and monitor the reliability and integrity of financial and operating information. It also allows the board of directors and/or audit committee to act as a powerful and proactive agent for organization self-regulation.

Thus, internal control:

- affects every aspect of an organization including staff, processes and operations;
- is integrated into the day-to-day operations and responsibilities of all staff;
- incorporates the qualities of good management;
- depends upon people and will succeed or fail depending on the attention people give to it; and
- must make sense within each specific operating unit's unique environment.

Why is Internal Control Important?

Internal control is important because it:

- promotes efficiency, reduces risks of asset loss, and helps ensure reliability of financial statements and compliance with laws and regulations;
- keeps the organization on course toward achievement of its mission;
- protects the organization by catching small mistakes before they become big problems;
- protects the organization by mitigating opportunities for innocent mistakes or intentional fraud that cause harm; and
- impacts every aspect of an organization – its people, processes, and physical structures.

Who has Responsibility for Internal Control?

Everyone in the organization has responsibility for ensuring the internal control system is effective. The strength of the system depends upon employees' attitude toward internal control and their attention to it. Executive management has the ultimate responsibility in this regard. Executive management sets the tone and must ensure that all personnel in the organization know their respective roles and responsibilities.

Management is responsible for developing detailed policies, procedures, and practices for their specific departmental operations and mission.

Limitations of Internal Control

An internal control system provides reasonable but not absolute assurance that an entity will achieve its objectives and mission. In any system of internal control there are inherent limitations. For example:

- human errors and poor judgment can cause mistakes (resulting from the pressure of decision making, limited information, etc.);
- controls can be circumvented by collusion of two or more people;
- management can intentionally override controls; and
- excessive costs can prevent management from implementing ideal controls.

Balancing Risk and Control (Cost vs. Benefit)

In an internal control system, risk caters to the possibility that an organization will not achieve its goals, operate effectively and efficiently, protect itself from loss, provide reliable financial data, and/or comply with applicable laws, regulations, policies and procedures. To achieve its goals and objectives, management needs to effectively balance risks and internal control. Control procedures need to be developed so that risk is decreased to an acceptable level.

Management may accept certain risks because the cost of preventing them cannot be justified. The cost of implementing a control compared to the benefit to be gained from the control must be carefully considered. Although prohibitive costs can prevent management from implementing ideal controls that does not mean that the control system ultimately will be ineffective. More control activities are not always better – staff perceptions of excessive controls can lead to negative views and affect their overall regard for the internal control system.

To achieve a balance between risk and controls, internal controls should be proactive, value-added, cost-effective and should decrease exposure to risk.

Consideration for the Design of Internal Controls

There is not a simple "one size fits all" when it comes to controls – an internal control system must be customized for the specific organization in view of:

- organizational size;
- organizational structure;
- nature of the business operations;
- diversity and complexity of operations;
- method of transmitting, processing, maintaining and accessing information; and
- applicable legal and regulatory requirements.

THE INTERNAL CONTROL FRAMEWORK

The five interrelated components of internal control are:

1. Control Environment
2. Risk Assessment
3. Control Activities
4. Information and Communication
5. Monitoring

1. Control Environment

The control environment serves as the foundation of any system of internal control and sets the tone for the entire organization.

The control environment is effectuated from the top of the organization, by management, and sets the tone for the entire organization, its operating structure and its communication of acceptable business practices and policies to staff. It establishes important control procedures such as authorization of activities, approval of transactions, and review of reconciliations. It also demonstrates the organization’s commitment to address prior audit recommendations through timely corrective action. The human resources department within an organization plays a critical role in effectuating the control environment directives of management and the interrelated principles enumerated below.

The concept and realization of a control environment is achievable through a focus on the following seven attributes of an organization’s control environment:

Integrity and Ethical Values

Integrity and ethical values refers to professional and personal codes of conduct and standards of behavior in the pursuit of an organization’s agenda. These are values established and agreed upon by the management of the organization and disseminated to staff as acceptable operational behaviors. Codes of conduct should be the source of guidance directing daily behavior and setting the minimum standards for that behavior. These values are particularly crucial in the governmental sector where the government is charged with properly managing public monies. Considerations for a strong ethical structure include:

- providing guidance for proper behavior through policy statements, codes of conduct, and behavioral example;

- removing or reducing temptations for unethical behavior;

- establishing methods for reporting ethical violations and consistently enforcing disciplinary policies when appropriate;

- establishing policies concerning ethical standards;

- performing background checks on employees who perform duties that are considered high risk; and

- communicating to employees the remedial actions and ramifications for not observing ethical standards.

Commitment to Competence

A commitment to competence ensures that staff and external support personnel are proficient and educated. It requires access to adequate on-going training, supervision, and the facilitation of professional memberships and development.

Examples of a commitment to competence include:

- clearly defined job duties and responsibilities based on management's analysis of the knowledge and skills needed to perform the job adequately;

- provision of continuous training and professional development necessary to maintain the job skills and qualifications needed to perform their duties; and

- regular monitoring and timely performance feedback to employees to ensure that the entity's objectives are being met.

Organizational Structure

Organizational structure is the legal and operational framework that management will adopt to guide its objectives, financial operations and measurements of achievement.

A well-functioning organizational structure will include:

- current and accurate organization chart that shows clear lines of management authority and responsibility;

- appropriate organizational structure considering the size and complexity of the organization;

- formal policies and procedures for all significant operations; and

- management support for internal control and response to internal and external audit recommendations.

Delegation of Authority and Responsibility

Management should authorize employees to perform activities and execute transactions only within defined parameters and include appropriate provisions for monetary thresholds, supervisory review and documentation requirements. Management should ensure that conditions for authorizations are clearly documented and communicated to ensure that significant transactions are approved and executed only by persons acting within the scope of their authority.

Relationship with Oversight Agencies, Boards of Directors and Audit Committees

Management's attitude toward and relationship with oversight agencies, Boards of Directors and Audit Committees demonstrate its commitment to the control environment it establishes. A positive relationship where acceptable corrective actions are implemented in a timely manner enforces the goals and objectives of management and communicates to all employees a positive attitude towards internal control.

Human Resources Policies and Procedures

Human resources departments play an important role in internal control in regard to areas such as proper hiring, orientation of new employees, evaluations, and disciplinary actions. As the tone at the top sends a message as to acceptable behaviors, meaningful human resource policies and procedures send a message to employees that management is serious in enforcing its rules.

2. Risk Assessment

Risk assessment is the process of identifying and analyzing relevant risks in order to manage and mitigate interruptions to essential business operations.

Paramount in the consideration of risk is the reliability of financial reporting of operations. Primary categories of risk are errors, omissions, delay, and fraud. Examples of risk include: assets that are not adequately safeguarded, production of unreliable reports, ineffective and inefficient operations, and noncompliance with regulations and laws.

An effective internal control system enables the agency to manage significant risks and monitor the reliability and integrity of financial and operating information.

The following steps should be considered during the risk assessment process:

Risk Identification

Management must identify, analyze, and manage risks that might negatively affect its objectives. Management should perform an evaluation to determine those areas and functions within the entity and each department that present a risk of errors, noncompliance, and fraud. Management must then institute controls to help mitigate the risks identified during the assessment.

There are many factors to consider when assessing risk, including: change in operating style, new employees, new or enhanced information technology systems, new programs and new and revised laws and regulations.

While trying to identify and evaluate risk, management should ask questions such as: what could go wrong, what is the worst case scenario, what would cause us to fail to meet our objectives, in what areas are we most vulnerable, and what assets do we need to safeguard.

There are many methods of identifying risk including: periodic management conferences, executive round tables, forecasting, strategic planning, and consideration of the findings from audits and other assessments.

Risk Management

Management must determine what the likelihood is of a certain risk leading to a financial loss or noncompliance with laws and regulations. Once a risk has been identified, management must decide how to manage the risk: accept the risk and not institute further controls, share the risk, reduce the risk by instituting controls, or avoid the risk by avoiding the function.

Uncontrolled risk can negatively impact the organization and prevent the organization from achieving its goals. Periodic re-evaluations of risk should be performed by management.

3. Control Activities

Control activities are the specific policies and procedures that are put in place to mitigate the risk of error, noncompliance, and fraud. These policies and procedures help to ensure that management's directives are being carried out. They should pertain to all levels of an entity and all functions within a particular department or area. Costs incurred for the design and implementation of control activities should be measured against the potential loss exposure.

Control activities cover a variety of primary functions within the control environment. Examples of such primary functions include:

Security of Assets

Specific control activities should be designed to minimize the risk of loss or misuse of assets and may include:

- utilizing unique user IDs and passwords to avoid unauthorized access;

- physical security of tangible and intangible assets such as cash, supplies, buildings, accounting records, blank checks, vehicles, equipment, gasoline, computers, etc.;

- backup for computer records and programs, utilizing a secure offsite facility;

- disaster recovery plans to keep the entity functioning after unexpected events; and

- performing periodic unannounced verifications of amounts, location, and condition of assets.

Segregation of Duties

Control activities should:

- prevent any one person from performing incompatible duties;

- require that the responsibility for operations be separate from the related record-keeping; and

- ensure that the three functions of authorizing, recording, and maintaining assets are separated.

In smaller organizations, when duties cannot be adequately separated compensating controls should be put in place. Examples of compensating control mechanisms include audit trails, reconciliations, exception reports, and supervisory review.

Authorization of Activities

Specific control activities should also be designed to define parameters for the execution of transactions. Examples include requiring authorization from management to a department or employee to execute transactions and requiring signature or electronic approval of the transaction by the employee designated with approval authority. Management should require that appropriate monetary thresholds be established and all documentation requirements be adhered to.

Approval, Verification and Reconciliation

Specific control activities should also be designed to ensure that a review of supporting documentation will confirm that the transaction is appropriate and accurate, and complies with all applicable laws, regulations, policies, procedures, etc. These specific control activities should:

- require that management specify those activities or transactions that require supervisory approval before they are performed;

- require supervisory approval to ensure that the transaction has been validated and conforms to established policies and procedures. Approval implies that the transaction has been reviewed, with substantive documentation supporting that the transaction is appropriate, accurate, and complies with applicable laws, regulations, policies, and procedures; and

- require that before a transaction is approved, there is a review of all supporting documentation, a questioning of any unusual items, and assurances that the available information supports the transaction.

Adequate Documentation

Specific control activities should also be designed to ensure that documents exist which support that the transaction specifies all relevant facts pertaining to dates, nature and scope, authorizations, approvals and verifications. These specific control activities should:

- require that transactions be supported by adequate documentation and that the documentation is as concise and clear as possible so that it is understood by all users;

- require the implementation of storage and retention policies that address the need for the secure physical storage of documents and the storage of backed-up electronic files; and

- require that the use of documents are periodically verified to ensure accountability and compliance with all pertinent laws and regulations including government contracting and granting requirements, and federal and state requirements concerning compliance with tax reporting, employment reporting, etc.

Information Processing

Specific control activities should be designed to ensure that appropriate policies and procedures regarding information technology are in place and adhered to by all personnel. These specific control activities should require that access within the computing environment be controlled by unique user passwords which are changed on a periodic basis.

Independent Performance Review

Specific control activities should be designed to ensure that internal controls are properly designed and working as intended. These control activities should recognize changes in operations that may make some controls unnecessary and identify new risks which may require the need for new controls. These specific control activities should:

- require that periodic reconciliations be performed;

- require the comparison of different sets of data to identify and investigate differences;

- require implementation of necessary corrective actions to ensure the accuracy and completeness of transactions;

- require management to review reports, statements, reconciliations and other information to ensure consistency and reasonableness; and

- require the comparison of information about current performance with budgets, forecasts, and prior periods to measure the extent to which objective goals are being achieved and to identify unexpected results or unusual conditions that require corrective actions.

4. Information and Communication

To achieve its goals and objectives, an organization needs relevant, reliable and timely information related to both internal and external events that can impact the organization and its mission.

Information and communication are essential throughout an organization. Current, accurate and reliable information about an organization's plans, control environment, risks, control activities, and performance must be communicated throughout an organization in a timely manner.

Information and communication help ensure that employees are aware of the organization’s goals and objectives, how they are to be accomplished, and who is responsible for the specific tasks needed to accomplish them. The information responsible for the specific tasks needed to accomplish them. The information and communication system should also provide managers with reports containing operational, financial, and compliance information to monitor progress toward accomplishing established goals and objectives and to allow managers to make appropriate decisions. Information and communication systems should include:

- written policies and procedures;
- mission statements, goals and objectives;
- organization charts;
- job descriptions and performance evaluations;
- training materials;
- periodic reports measuring the entity's progress towards accomplishing its goals and objectives;
- internal and external audit reports; and
- financial reports.

Information and communication systems can be formal or informal. Formal information and communication systems should provide for input and feedback relative to operations, financial reporting and compliance objectives. Similarly, informal conversations with clients, suppliers, regulators, and employees often provide critical information needed to identify risks and opportunities.

Information

Reliable and relevant information from both internal and external sources must be identified, captured, processed, and communicated to the people who need it in a form and time frame that is useful. Information systems should produce reports containing operational, financial, and compliance-related information that make it possible to operate and control an organization. The quality of system-generated information that is produced affects management's ability to make appropriate and timely decisions. Bad information results in bad decisions.

Communication

Communication facilitates an understanding of individual roles and responsibilities. Information and communication channels support complete, correct and timely financial reporting by making all relevant internal process instructions and policies accessible to all employees. Internal communications may occur through meetings or day-to-day activities. Regular updates regarding changes in accounting policies and reporting and disclosure requirements are critical to ensure that everyone in the organization works under the same rules and regulations and understands their duties and expectations.

The following information should be communicated within an organization:

- organizational performance data;
- operational data;
- financial data; and

- employee performance data.

Communication may take the following forms:

- performance and management systems;
- information systems;
- policy and procedure manuals;
- management directives;
- memos and e-mails;
- internet and intranet; and
- speeches and briefings.

Characteristics of effective organizational communication include:

- relevant internal and external information on operational performance is provided to management;
- the information provided is current, accurate, complete and timely;
- information is shared with the appropriate staff members at the right time;
- management is receptive to employee suggestions; and
- there are appropriate channels through which to report improprieties.

5. Monitoring

Monitoring is the assessment of internal control performance over time. It is accomplished by, for example, self-assessments, peer reviews, and internal audits.

The purpose of monitoring is to determine whether internal controls are adequately designed, properly executed and effective. Internal controls are adequately designed and properly executed if all five internal control components (Control Environment, Risk Assessment, Control Activities, Information & Communication, and Monitoring) are present and functioning as designed. Internal control is effective if management and interested stakeholders have reasonable assurance that:

- an operation's objectives are being achieved;
- financial statements are being prepared reliably; and
- applicable laws and regulations are being complied with.

Monitoring helps to ensure that control activities and other actions that effect internal control are carried out properly, effectively and in a timely manner. Ongoing monitoring activities include various management and supervisory activities that evaluate and improve the design, execution and effectiveness of internal control. Separate evaluations, on the other hand, such as self-assessments and internal audits, are periodic evaluations of internal control components that result in a formal report addressing the adequacy and effectiveness of internal control.

Department employees perform self-assessments. Internal auditors perform internal audits and provide an independent appraisal of internal control.

Monitoring should include routine financial and program activities such as, ongoing supervision, reconciliations, comparisons, performance evaluations, and status reports. Internal control systems should generally be designed to ensure that ongoing monitoring occurs in the normal course of operations. Proper monitoring ensures that controls continue to be adequate and function properly.

Deficiencies found during ongoing monitoring or through separate evaluations should be communicated to the individual responsible for the function and also to top level management, the Board of Directors, the Audit Committee, or those charged with corporate governance.

Monitoring of internal control should include policies and procedures for ensuring that the findings of audits and other reviews are promptly resolved. Managers should:

- promptly evaluate findings from audits and other reviews, including those showing deficiencies and recommendations reported by auditors and others who evaluate the agency's operations;

- determine proper actions in response to findings and recommendations from audits and reviews; and

- complete, within established time frames, all actions that correct or otherwise resolve the matters brought to management's attention.

Monitoring should focus on the following major areas:

Control Activities

Control activities are established to prevent or reduce the risk of problems occurring. If these activities fail, the department becomes exposed to risk. Therefore, management should establish procedures which monitor the effectiveness of control activities and the use of control overrides. Effective monitoring gives management the opportunity to identify and correct any control activity deficiencies or problems and to minimize the impact of unfavorable events.

Mission

Monitoring activities should include the development and review of operational data that allow management to determine whether the department is achieving its mission. This can be achieved through a periodic comparison of operational data to the department'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 ensure that the staff is competent, that adequate training is provided and that management styles and philosophies foster accomplishment of the department's mission.

Communication

Managers should periodically verify that employees 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 encourages reporting of both positive and negative information.

Risks and Opportunities

Managers should also monitor the department's internal and external environment to identify any changes in risks or opportunities for improvement. If changes are identified, managers should take appropriate action to address these new conditions. Management should recognize that delays in responding to risks could result in damage to the department. A slow response to changes in risk may result in lost revenue or unattained cost savings.

PART III

INFORMATION TECHNOLOGY

Information Technology (IT) consists of the development, implementation, support and management of computer-based information systems, particularly software applications and computer hardware. IT controls are a subset of an entity's internal control system and consist of specific activities, performed by persons or systems, designed to ensure that business objectives are met. IT control objectives relate to the confidentiality, integrity, and availability of data and the overall management of the entity's IT function. IT controls are often described in two categories: general and application.

General Controls

IT general controls include the policies, procedures, practices and organizational structures designed to provide reasonable assurance that systems operate as intended, business objectives are achieved, output is reliable, and undesired events are prevented or detected and corrected. IT general controls include controls over the computer and network operations, access to programs and data, systems software acquisition and maintenance, and program development and changes.

General controls pertain to all information systems (mainframe, network, and end-user environments).

Physical security encompasses the area containing system hardware, including the wiring used to connect systems, supporting devices and backup systems. Logical security uses technology to allow individuals access to information and systems based on who they are and what their role is within the organization. Access to information technology resources should be restricted to those individuals with a need for such access.

IT general controls may include:

- Changes in management procedures - designed to ensure changes meet business requirements and are authorized;

- Document control procedures - designed to protect the integrity of program codes;

- Software development standards - designed to ensure IT projects are effectively managed;

- Security policies, standards, and processes - designed to secure access to information and systems based on business need;

- Incident management policies and procedures - designed to address operational processing errors;

- Technical support policies and procedures - to help users perform more efficiently and report problems;

- Hardware/software configuration, installation, testing, and management standards controls - designed to ensure consistent acquisition, implementation, maintenance, and testing of new systems and the modification of existing systems; and

- Disaster recovery/backup procedures - designed to enable continued processing despite adverse conditions.

Application Controls

Application controls pertain to the processing of data within software applications.

IT application controls are performed automatically by systems designed to ensure the complete and accurate processing of data. Such controls vary based on the business purpose of the specific application. These controls also may help ensure the privacy and security of data transmitted between applications and may help to ensure that transactions that occur, are authorized, and are completely and accurately recorded and processed. Examples include edit checks of input data and numerical sequence checks.

IT application controls may include:

- Completeness checks that ensure all records were processed from initiation to completion;

- Validity checks that ensure only valid data is inputted or processed;

- Identification controls that ensure all users are uniquely identified;

- Authentication controls that provide an authentication mechanism (e.g., user name and password) in the application system;

- Authorization controls that ensure only approved business users have access to the application system; and

- Input controls that validate data input against applicable criteria to identify errors and ensure data integrity.

FINANCIAL MANAGEMENT SYSTEMS

Financial management is the process of managing an entity's financial resources, including its budgeting, accounting and financial reporting. A financial management system can be automated or manual, and maintained in-house or through the services of an outside consultant.

The accounting system consists of financial records and other relevant fiscal information. This includes the financial plan, budget, payroll and other financial processes of the business. The purpose of the system is to accumulate data and provide decision makers with information that is timely, accurate, and complete.

An effective accounting system identifies and records all valid transactions, describes transactions in sufficient detail to permit proper classification for financial reporting, measures the value of transactions in a manner that permits proper monetary recording, records transactions in the proper accounting period and presents transactions properly in financial statements or other financial documents.

COMPLIANCE

Government entities and business organizations are required to adhere to numerous laws and regulations mandated by federal, state and local governmental authorities. These include financial, procurement, labor and employment, payroll, tax, advertising, and antitrust laws and regulations.

Internal controls should include appropriate measures to ensure compliance with all pertinent laws, rules and regulations affecting the organization. Management must ensure that it has an effective process to monitor new rules and regulations including those rules and regulations that apply to a new business activity or venture, or to new or unique funding streams and initiatives. Some sources of state and federal rules and regulations along with some pertinent federal statutes are noted below. Refer to the references section at the conclusion of this guide for specific pertinent web sites.

Sources of State Rules and Regulations include:

- Governor's Executive Orders;
- Departmental Rules, Regulations, and Policies; and
- Department of the Treasury Circular Letters.

Sources of Federal Rules and Regulations include:

- U.S. Office of Management and Budget guidance; and
- Federal departmental web sites.

Pertinent Federal statutes include:

- Davis Bacon Act;
- Buy American Act;
- False Claims Act; and
- Federal whistleblower protection statutes.

FRAUD AWARENESS

According to Statement on Auditing Standards (SAS) No. 99, Consideration of Fraud in a Financial Statement Audit, management is responsible for designing and implementing systems and procedures for the prevention and detection of fraud and, along with the board of directors, for ensuring a culture and environment that promotes honesty and ethical behavior.

According to Black's Law Dictionary, fraud is "a false representation of a material fact, whether by words or by conduct, by false or misleading allegations, or by concealment of that which should have been disclosed, which deceives another so that he acts, or fails to act, to his detriment."

Common anti-fraud measures include external audits, internal audits, fraud training, surprise audits, and the establishment of a hotline to report allegations of fraud.

The following three elements may be present when fraud occurs: opportunity, motive (typically financial), and ability to rationalize. Without these three elements, fraud is unlikely to occur.

- **Motive -** some kind of pressure or perceived pressure, typically financial, such as the need to pay for an extraordinary expense (e.g., medical debt, gambling debt). Motive could also be greed, revenge, thrill seeking, etc.
- **Opportunity -** typically caused by the ability to circumvent internal controls or by internal control weaknesses.
- **Rationalization -** some excuse or perceived validation for actions.

The main types of fraud are:

- Management Fraud
- Employee Fraud
- Vendor Fraud

Management Fraud frequently involves top management's manipulation of financial statements.

Employee Fraud involves the embezzlement of organizational assets by employees.

Vendor Fraud involves overcharging for goods, shipping inferior goods or not shipping goods at all even though payment has been received.

Specific examples of fraud include:

- Theft or misappropriation of funds, supplies, computer software, intellectual property, or other resources;
- Fictitious revenues or disbursements;
- Check tampering (e.g., forged endorsement, altered payee, concealed checks);
- Fictitious write-offs and refunds;
- Fictitious vendor or employee payments;
- False statements;

- False overtime;
- False request for reimbursement;
- Forgery or alteration of documents;
- Bribery or attempted bribery;
- Invoice kickbacks;
- Bid rigging;
- Illegal gratuities;
- Unauthorized use of records or access to information systems, including unauthorized sharing of computer security clearances;
- Unauthorized alteration, manipulation, or destruction of computer files and data;
- Falsification of reports to management or external agencies;
- Conflicts of interest that provide a personal benefit or advantage while compromising the public interest;
- Improper handling or reporting of financial transactions;
- Concealed liabilities and expenses, and improper asset valuations;
- Inaccurate employment credentials;
- Authorizing or receiving compensation for hours not worked;
- Incurring obligations in excess of appropriate authority;
- Payroll and sick time abuses; and
- Willful violation of laws, regulations, policies or contractual obligations.

Fraud indicators include:

- Unsupported or unauthorized transactions;
- Missing or altered documents;
- Inconsistent, vague, or implausible responses from management or employees arising from inquiries or analytical procedures;
- Denial of access to records, facilities, employees, or others from whom audit evidence might be sought;
- Unusual delays in providing requested information;
- Numerous complaints about management or staff;
- Significant transactions involving related-parties (individuals with personal or business relationships);
- Inadequate or absent internal controls;

- Analytical anomalies;
- Unexplained inventory shortages;
- Purchases in excess of needs;
- Excessive voided transactions; and
- Cash shortages

Management can take steps to deter the occurrence of fraud and mitigate associated losses. A critical component of this effort is the proper education of employees concerning fraud awareness. A control environment that promotes the prevention and detection of fraud will reinforce management's intent in this regard. Employees also must understand that there are consequences associated with the commission of fraudulent acts, including disciplinary and criminal consequences.

The perception of the possibility of detection is the biggest deterrent to fraud.

All staff are responsible for reporting fraud, waste, and abuse. Timely reporting is important. Many states have such reporting mechanisms. For example, in New Jersey, the Office of the State Comptroller has a toll-free Government Waste and Mismanagement Hotline (1-866-OSC-TIPS). At the federal level there are a number of federal department and inspector general websites that have similar reporting mechanisms.

GLOSSARY

ABUSE

To use wrongly or improperly.

ACCOUNTABILITY

Recognition that one is answerable for the outcome regardless of the cause.

APPROVAL

Confirmation of employee decisions, events, or transactions based on a review.

AUDIT RISK

A combination of the risk that material errors will occur in the accounting process and the risk that errors will not be discovered by audit tests. Audit risk includes uncertainties due to sampling (sampling risk) and other factors (non-sampling risk).

AUTHORIZATION

The power management grants employees to carry out certain duties based on approval received from supervisors.

COLLUSION

A secret agreement between two or more persons or entities to deceive, mislead, or defraud others of their legal rights, or to obtain an objective forbidden by law typically by defrauding or gaining an unfair advantage.

CONTROL ACTIVITIES

Policies, procedures, techniques, and mechanisms that help ensure that management's directives to mitigate risks identified during the risk assessment process are carried out. Control activities occur at all levels of the agency. They include a wide range of diverse activities, such as approvals, authorizations, verifications, reconciliations, performance reviews, security activities, and the production of records and documentation. Control deficiencies exist when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements in a timely manner.

CONTROL ENVIRONMENT

The control environment sets the tone of the organization, influencing the consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. The control environment is greatly influenced by the extent to which individuals recognize that they will be held accountable.

CONTROL RISK

The risk that a material error in a balance or transaction class will not be prevented or detected on a timely basis by the internal control system.

DEFALCATION

An amount of funds misappropriated by a person trusted with its charge; also, the act of misappropriation.

DETECTION RISK

The risk that audit procedures will lead to a conclusion that material errors do not exist when in fact such errors do exist.

DETECTIVE CONTROLS

Detective controls provide evidence that a loss has occurred, but do not prevent a loss. Examples include review and analyses, variance analysis, reconciliations, physical inventories, and audits.

EFFECTIVENESS

Ability of the entity to accomplish its goals.

EFFICIENCY

Maximizing the best use of resources.

FINANCIAL STATEMENTS

The formal record of the financial activities of a business, person, or other entity. For a business enterprise, the financial statements typically include the Balance Sheet, Income Statement, Statement of Retained Earnings, and Statement of Cash Flows.

FRAUD

A misrepresentation or concealment with reference to some fact material to a transaction that is made with knowledge of its falsity or with reckless disregard of its truth or falsity and with the intent to deceive another and that is reasonably relied on by the other who is injured.

GENERALLY ACCEPTED ACCOUNTING PRINCIPLES (GAAP)

Refers to the standard framework of guidelines for financial accounting which are generally known as accounting standards. GAAP includes the standards, conventions, and rules accountants follow in recording and summarizing transactions, and in the preparation of financial statements.

GENERALLY ACCEPTED GOVERNMENT AUDITING STANDARDS (GAGAS)

Commonly referred to as the **"Yellow Book**," these standards are produced by the U.S. Government Accountability Office (GAO). The standards apply to both financial and performance audits of government agencies. Five general standards are included: Independence/Due Care/Continuing Professional Education/Supervision/Quality Control.

INFORMATION MANAGEMENT SYSTEM

Consists of the methods and records established to record, process, summarize, and report the operations and performance of the entity.

INHERENT LIMITATIONS

Limits of all internal control systems include human judgment, resource constraints, the need to balance the costs of the control in relation to the expected benefits, the reality that breakdowns will and can occur, the possibility of management overrides, and collusion.

INHERENT RISK

The risk of a material misstatement in unaudited information assuming the absence of internal control procedures.

MALFEASANCE

Performance by a public official of an act that is legally unjustified, harmful, or contrary to law.

MANAGEMENT INTERVENTION

Management's actions to override prescribed policies or procedures for legitimate purposes such as a non-recurring event or non-standard transaction or event.

MANAGEMENT OVERRIDE

Management's overriding of prescribed policies or procedures for illegitimate purposes with the intent of personal gain.

MATERIALITY

Measure of the estimated effect that the presence or absence of an item of information may have on the accuracy or validity of a statement. It cannot be expressed in a simple calculation and is determined by a person's reliance on the information and whether an omission or misstatement of the information would influence the readers' opinion.

MATERIAL WEAKNESS

A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting such that there is a reasonable possibility that a material misstatement of the company's annual or interim financial statements will not be prevented or detected on a timely basis.

MISFEASANCE

Improper and unlawful execution of a normally lawful act; deliberate and dishonest abuse of power; wrongful performance of a normally lawful act.

MONITORING

Internal control monitoring should assess the quality of performance over time and ensure that the findings of audits and other reviews are promptly resolved.

ORGANIZATIONAL STRUCTURE

The organizational structure provides the overall framework for planning, directing, and controlling operations. This structure defines the form and nature of the organization, as well as management functions and reporting relationships. Authority and areas of responsibility should be appropriately assigned. The organizational chart should delineate clear lines of authority.

POLICY

Management's directive of what is required to effect control.

PREVENTIVE CONTROLS

Preventive controls attempt to deter or prevent undesirable events from occurring. Examples include segregation of duties, proper authorization protocols, requiring adequate supporting documentation, and maintaining physical control over assets.

PROCEDURE

An action that implements a policy.

REASONABLE ASSURANCE

The concept that internal control, regardless of how well designed, cannot guarantee an organization's objectives will be met since inherent limitations will always exist.

RELIABILITY

A high degree of certainty and predictability for a desired outcome. Reliability for financial reporting refers to the accuracy of financial statement balances and adequate and complete disclosure.

REPORTABLE CONDITION

Matters coming to the auditor's attention that are communicated to the audit committee because they are significant deficiencies in internal control which could adversely affect the ability to record, process, summarize, and report financial data.

RISK

The probability that a transaction or event will adversely affect the organization.

RISK ASSESSMENT

The process wherein management identifies the risks (internal and external) that could impede the efficient and effective achievement of the organization's objectives. Once the risks are identified, management formulates an approach for risk management and decides upon the internal control activities required to mitigate those risks.

SAMPLING RISK

The possibility that conclusions reached from a sample may not represent correct conclusions for the entire population.

SEGREGATION OF DUTIES (also referred to as separation of duties)

Division of key duties and responsibilities among different people to reduce opportunities for any individual to be in the position to commit and conceal errors (intentional or unintentional) or perpetrate fraud in the normal course of their duties.

SIGNIFICANT DEFICIENCY

A control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report external financial data reliably in accord with Generally Accepted Accounting Principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements (that is more than inconsequential) will not be prevented or detected.

STATEMENTS ON AUDITING STANDARDS

Commonly abbreviated as SAS, these statements provide guidance to auditors on Generally Accepted Auditing Standards in regards to auditing an entity and issuing an audit report.

SUPERVISION

Ongoing oversight, management, and guidance of an activity by designated employees to help ensure that the results of the activity achieve established objectives.

VERIFICATION

Determination of the completeness, accuracy, authenticity, and/or validity of transactions, events, or information. It is a control activity that allows management to confirm activities are being performed in accordance with stated directives.

WASTE

Useless consumption or expenditure. An expenditure that is extravagant or imprudent.

REFERENCES

A123 Management and Accountability and Control

www.whitehouse.gov/omb/circulars/a123/a123.html

AICPA – Journal of Accountancy – Understanding Internal Controls

www.journalofaccountancy.com/Issues/2009/Sep/White+Paper+Understanding+Internal+Control+and+Internal+Control+Services.html

COSO

www.coso.org/

GAO – Federal Information Systems Controls Audit Manual (FISCAM)

www.gao.gov/new.items/d09232g.pdf

GAO – Generally Accepted Government Auditing Standards (The Yellow Book)

www.gao.gov/govaud/ybk01.htm

GAO – Internal Control Management Evaluation Tool

www.gao.gov/new.items/d011008g.pdf

GAO – Standards for Internal Control (The Green Book)

www.gao.gov/archive/2000/ai00021p.pdf

National Procurement Fraud Task Force – A Guide to Grant Oversight and Best Practices for Combating Fraud

www.nsf.gov/oig/grant_fraud.pdf

New Jersey ARRA Task Force Resources

www.nj.gov/taskforceresources

New Jersey Department of Treasury – Circular Letters

www.state.nj.us/infobank/circular/circindx.htm

REFERENCES (Continued)

New Jersey Executive Orders

www.state.nj.us/infobank/circular/eoindex.htm

New Jersey Office of State Comptroller – Best Practices for Awarding Service Contracts

www.nj.gov/comptroller/news/docs/service_contracts_report.pdf

New York State Internal Control Association (NYSICA)

www.nysica.com

New York State – Management Responsibility for Internal Controls

www.osc.state.ny.us/localgov/pubs/lgmg/managementsresponsibility.pdf

New York State – **Standards for Internal Controls**

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

U.S. Government Accountability Office (GAO)

www.gao.gov

U.S. Department of Defense – Fraud Awareness Training

www.dodig.mil/Inspections/APO/fraud/Index.htm

U.S. Office of Management and Budget (OMB)

www.whitehouse.gov/omb/