Internal Control Guide & Resources

Section 1- Internal Control Overview

Internal control involves all processes that assure achievement of an organization's objectives and that controls risks to an organization. It is a fundamental element of the Sarbanes-Oxley Act of 2002.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control Integrated Framework is the most widely used internal control framework around the world. COSO is a voluntary private sector initiative dedicated to improving organizational performance and governance through effective internal control, enterprise risk management, and fraud deterrence. In May 2013, COSO released an update to modify their original framework to maintain relevance with current and future business environments. The updated framework applies to public companies, privately held companies, not-for-profit agencies and governmental entities. This Internal Control Guide provides guidance based upon this updated framework.

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 relating to operations, reporting, and compliance." A more in depth review of the categories of objectives is provided below:

- *Operations Objectives* – These pertain to effectiveness and efficiency of the entity's operations, including operational and financial performance goals, and safeguarding assets against loss.
- *Reporting Objectives* – These pertain to internal and external financial and non-financial reporting and may encompass reliability, timeliness, transparency, or other terms set forth by regulators, standard setters, or the entity's policies.
- *Compliance Objectives* – These pertain to adherence to laws and regulations to which the entity is subject.

Management sets these objectives in specific and measurable terms before designing an entity's internal control system. Setting objectives establishes the criteria for setting controls which keep activities within the boundaries of what is allowed or expected by management. The process of setting objectives may be included as part of the strategic planning process.

Internal control is comprised of the plans, methods, policies, and procedures used to fulfill the mission, strategic plan, goals, and objectives of the organization. Management responsibilities for internal controls are met when:

- Programs and functions achieve their intended results (effective)

- Resource use is consistent with the agency mission (efficient)
- Laws and regulations are followed(compliance)
- Accurate and timely information is prepared (reliable reporting)

All objectives, controls, and desired levels of performance must be communicated to all personnel to ensure accountability in an internal control system. Everyone in the work place has a role in making sure that internal controls are working. It is up to mangers to set them up and check that they are working, but unless every employee is aware of his/her responsibilities in the process, the control system will not be completely functional.

The following sections of OIA’s Internal Control Guide will discuss the five integrated components of internal control and the 17 principles associated with them, as established by COSO’s updated framework. Each component and principle is described and the applicability to management is explained.

Section 2- The Five Components of Effective Internal Controls

Internal Control Environment

The control environment is the foundation for an internal control system. It includes the overall attitude and actions of management regarding the importance of controls in their organization. Internal controls are likely to function well if management believes that those controls are important and communicates that view to employees at all levels.

COSO's updated internal control framework identifies five principles associated with the control environment:

1. The oversight body and management should demonstrate a commitment to integrity and ethical values.
2. The oversight body should oversee the entity's internal control system.
3. Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.
4. Management should demonstrate a commitment to attract, develop, and retain competent individuals.
5. Management should evaluate performance and hold individuals accountable for their internal control responsibilities.

The implementation of these five principles is crucial to the implementation and operating effectiveness of the internal control environment.

For information regarding how to analyze your agency's internal control environment, refer to Section 3 of OIA's Internal Control Guide "How to Analyze Your Agency's Control Environment."

Risk Assessment

A risk is anything that endangers the achievement of an objective. The risk assessment process is used to identify, analyze, and manage the potential risks that could hinder or prevent an agency from achieving its objectives. Risk increases during a time of change, for example, turnover in personnel, rapid growth, or establishment of new services. Other potential high risk factors include complex programs or activities, cash receipts, direct third party beneficiaries, and prior problems.

COSO's updated internal control framework identifies four principles associated with this internal control component:

6. Management should define objectives and risk tolerances.

7. Management should identify, analyze, and respond to risks related to achieving the defined objectives.

8. Management should consider the potential for fraud when identifying, analyzing, and responding to risks.

9. Management should identify, analyze, and respond to significant changes in the internal control system.

For information regarding how to conduct your own risk assessment, refer to Section 4 of OIA's Internal Control Guide "How to Conduct a Risk Assessment."

Internal Control Activities

Internal control activities are nothing more than policies, procedures, and the organizational structure of an organization. Organizations establish policies and procedures so that identified risks do not prevent an organization from reaching its objectives. Clearly identified activities minimize risk and enhance effectiveness.

Internal control activities can be either preventive, for example, requiring supervisory sign off, or detective, for example reconciling reports. Excessive controls should be avoided, as they can be as harmful as excessive risk and result in increased bureaucracy and reduced productivity.

COSO's updated internal control framework identifies three principles associated with this internal control component:

10. Management should design control activities to achieve objectives and risk responses.

11. Management should design control activities for the entity's information system.

12. Management should implement control activities.

For further information and examples of Internal Control Activities, refer to Section 5 of OIA's Internal Control Guide "Internal Control Activities- Best Practices.

Information and Communication

Information must be reliable to be of use and it must be communicated to those who need it. For example, supervisors must communicate duties and responsibilities to the employees that report to them and employees must be able to alert management to potential problems. Information must be communicated both within the organization and externally to those outside, for example, vendors, recipients, and other applicable parties. Communication must also be ongoing both within and between various levels and activities of the agency.

COSO's updated internal control framework identifies three principles associated with the information and communication component:

13. Management should use quality information.
14. Management should internally communicate the necessary quality information.
15. Management should externally communicate the necessary quality information.

For further information and examples of Internal Control Activities, refer to Section 6 of OIA's Internal Control Guide "Information and Communication."

Monitoring

After internal controls are put in place, their effectiveness needs to be periodically monitored to ensure that controls continue to be adequate and continue to function properly. Management must also monitor previously identified problems to ensure that they are corrected.

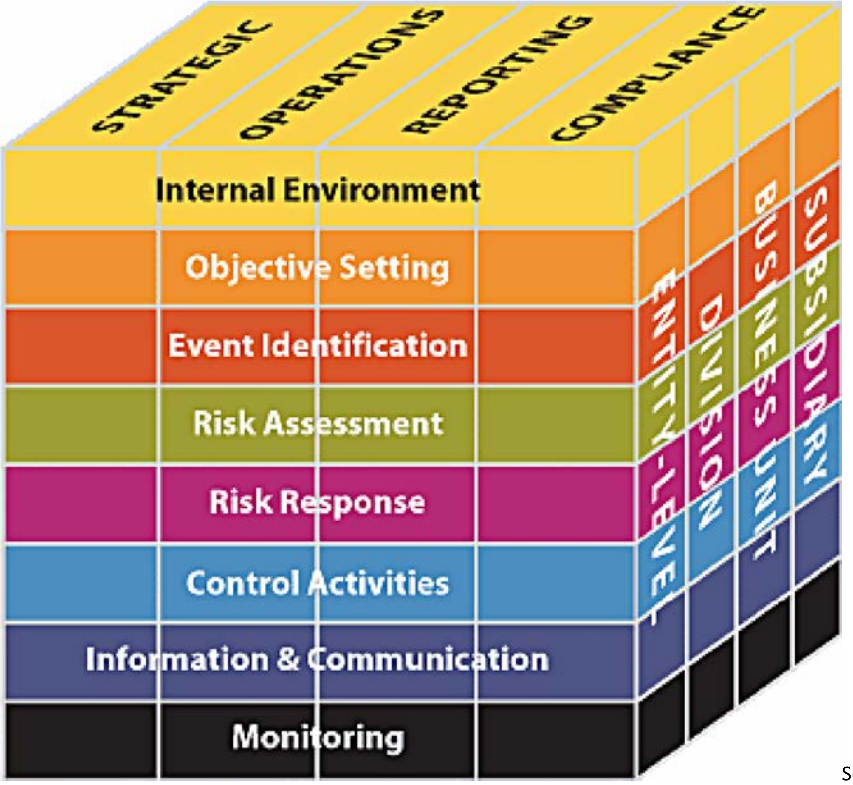
COSO's updated internal control framework identifies two principles associated with this internal control component:

16. Management should establish monitoring activities to monitor the internal control system and evaluate the results.

17. Management should ensure identified internal control deficiencies are remediated on a timely basis.

For further information and examples of Internal Control Activities, refer to Section 7 of OIA's Internal Control Guide "How to Monitor Effectively."

The internal control system is a dynamic and integrated process in which each of the five components described above impact the effectiveness of the other components. A relationship exists not only between the components, but also the objectives and the agency's organizational structure. COSO's depiction of this relationship is provided below:



Source: Compliancy Software

Due to this integrated relationship, it is essential that management have a plan to implement each of the 17 principles associated with the five internal control components. The following sections of OIA's Internal Control Guide have been written and designed to assist management in evaluating and carrying out this objective.

Internal Control Guide & Resources

Section 3- How to Analyze & Improve Your Agency's Control Environment

The control environment of a state agency sets the tone of the organization and influences the effectiveness of internal controls within the agency. The control environment is the foundation of the COSO internal control framework. Managers must evaluate the internal control environment in their own unit and department as the first step in the process of implementing internal controls.

Analyze the Control Environment

- **Attitude:** Review the unit's control environment including your and any subordinate managers' attitudes and actions. If a specific procedure requires constant exceptions, you are better off changing or eliminating the procedure than establishing an attitude of "rules are made to be broken." Whether you realize it or not, as a manager, you set an example by your behavior. If managers make exceptions to their own procedures whenever they find themselves inconvenienced, staff and contractors will feel they too can also make exceptions whenever they want.
- **Supervision:** Departments with the best control environment attempt to hire qualified individuals while making an effort to retain skilled employees. Their managers train new and current staff to excel at their jobs and to use appropriate internal controls in all areas. They assist their staff by furnishing tools such as job descriptions and policy and procedure manuals that clearly communicate responsibilities and duties. They provide sufficient but not excessive supervision, reviewing to the extent necessary. While they allow as much autonomy as possible to competent, experienced staff, they continue to approve work at critical points to ensure that work flows as intended.
- **Structure:** Managers should develop an organizational structure that clearly defines supervisory responsibilities and chains of command. The structure should also take into account the need to separate certain duties. This structure should be documented through organizational charts made available to all staff.

Your Responsibilities

In your leadership role, you should make every effort to:

- Create a positive control environment
- Create an open workplace where concerns and comments are welcomed and acted upon
- Ensure all duties are performed in an ethical and professional manner

- Endorse and actively support agency systems of internal controls and operational processes
- Communicate and provide training on the importance of delivery of agency objectives and services, and
- Actively encourage agency employees to adhere to the entire Rhode Island code of ethics.

Part of your responsibility for your agency's financial internal controls and processes will require you to be involved in:

- Establishing appropriate internal controls and procedures that allow for the efficient, effective and economical management of the agency's financial resources
- Clearly defining key responsibilities and delegated authority levels
- Evaluating performance on a routine basis and ensure individual accountability for responsibilities
- Completing agency risk assessments and implementing appropriate offsetting controls and processes, with particular attention, where necessary, to areas with potential for fraud
- Establishing processes and standards for reporting on operational and financial performance
- Establishing appropriate lines of reporting
- Monitoring the effectiveness of agency controls and processes through results reported to executive management, and
- Ensuring ongoing training for staff about financial internal controls and processes.

Staff Responsibilities

Staff also needs to play a role in ensuring internal controls are operating effectively to achieve the agency's objectives and services. If a staff is aware of any deficiencies in internal controls he/she is responsible to report it to management.

Control Objectives to Implement

1. Management emphasizes the importance of internal control through its attitude, actions, and values, and communicates this tone to all employees.
2. Management adheres to a code of conduct and other policies regarding acceptable business practices, conflicts of interest, or expected standards of ethical and moral behavior, and communicates these policies to all employees.
3. Management takes appropriate disciplinary action in response to departures from approved policies and procedures or violations of the code of the conduct.
4. A strategic plan and mission statement are in place to provide guidance and assistance to management.
5. Organizational structure is defined, updated, and communicated to all employees with adequate and appropriate reporting relationships.

6. Qualified and trained personnel are hired to help ensure control procedures are followed and resources used efficiently.
7. Current job descriptions are established detailing the responsibilities and qualifications for each position.

After you have taken a more proactive approach to your responsibilities and implemented the above control objectives, it would be helpful to perform another analysis of your agency's control environment.

Analysis of Control Environment- Tips to Remember

- Do not focus internal control tests exclusively on activity-level controls; the control environment needs to be evaluated and tested on a routine basis.
- Establish a benchmark to gauge internal control effectiveness.
- Use different testing techniques to gather information about the control environment from a broad range of personnel.

Section 4- How to Conduct a Risk Assessment

Performing risk assessments assists managers in prioritizing the activities where controls are most needed. Keep in mind that the objective of a risk assessment is to attain a “reasonable” level of assurance that the organization’s financial and compliance goals will be achieved. Trying to attain an absolute level of assurance is not possible due to the following reasons:

- It is cost-prohibitive. The objective is to find an optimal level of control for an acceptable level of risk.
- Management can potentially bypass or override the internal controls.
- Employees may collude with each other.
- Human error may occur.

When conducting a risk assessment, the following steps should be followed:

1. Identify all significant activities or processes for which you are responsible. To simplify this task, we suggest grouping activities of the program or function into control cycles. A **control cycle** is a group of actions used to initiate and perform related activities. Control cycles provide the focal point for evaluating internal controls.

2. Make sure that the activities (or processes) for which you are responsible have clear and measurable objectives.

3. Identify the inherent risks for each activity/process.

   a. Examples include complex programs or activities, cash receipts, providing services through sub-recipients or vendors, direct third party beneficiaries, and prior problems. Activities with inherent risk have a greater potential for loss from fraud, waste, unauthorized use, or misappropriation due to the nature of the activity or asset. Cash, for example, has a much higher inherent risk for theft than a stapler.

   b. Determine if any of these situations apply to the activity/process:

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

ii. *Third party beneficiaries* are more likely to fraudulently attempt to obtain benefits when those benefits are similar to cash (for example food stamps).

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

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

v. *Unresponsiveness to identified control weaknesses* by prior auditors often indicates that future weaknesses are likely to occur.

4. Ask yourself the following questions:

- What could go wrong?
- How could we fail?
- What must go right for us to succeed?
- Where are we most vulnerable?
- What assets do we need to protect?
- How could someone steal from the department?
- How could someone disrupt our operations?
- What information do we rely upon the most?
- What do we spend the most money on?
- How do we collect money?
- What decisions require the most judgment?
- What activities are regulated?
- What is our greatest legal exposure?

5. Review changes. The risk to reaching objectives increases dramatically during a time of change. Consider various external and internal risk factors such as:

- Changing economic and political conditions
- New technology
- New accounting standards
- Changes in personnel, for example after a new administration
- New or modified information systems
- New programs or services
- Reorganization within or between state agencies
- Rapid growth
- Increased delegation of spending authority
- Moving to a new location

6. For each identified risk, evaluate the potential impact (minor, moderate, or severe) on your agency that would occur if such an event were to happen. Then estimate the likelihood (unlikely, likely, very likely) that such an event might happen.

7. Based on these two estimates, rank the risks so that you can identify which risks should be addressed first. Ask yourself how your agency can best manage the risks you have identified.

Risk Evaluation

		Impact		
		Minor	*Moderate*	*Severe*
Likelihood	*Very Likely*	Medium Risk	High Risk	Extreme Risk
	Likely	Low Risk	Medium Risk	High Risk
	Unlikely	Low Risk	Low Risk	Medium Risk

Section 5- Internal Control Activities & Best Practices

Managers must establish internal control activities that support the five internal control components discussed in Section 2 of the Internal Control Guide.

There are two main types of control activities. Controls can be either **preventive**, for example, requiring supervisory sign-off before an item is purchased, or **detective**, for example reconciling bank statements to ensure that all payments are appropriate.

Examples of key internal control activities that agencies should establish and incorporate in an internal control structure are described in the following sections.

Authority

The various stages of a transaction or activity should be carried out and approved by employees acting within their range of knowledge and proper span of control. These stages include the processes of recording, approving, and reconciling.

Best Practices:

- Policies and procedures should clearly identify which individuals have authority to initiate, submit, reconcile, view or approve different types of transactions.

- Employees should be properly trained and informed of departmental procedures related to internal controls. Individuals should have firsthand knowledge of the transactions being approved, or they should review supporting documentation to verify the validity and appropriateness of transactions.

- The workflow process should stress timely authorizations as well as timely processing of transactions following approval. Workflow is an important aspect of good internal controls. Time lags between approval and processing provide opportunities for altered documents and potential fraud.

Document Internal Controls and Maintaining Other Types of Documentation

Documenting policies and procedures is especially important because one truth of our time is that change happens constantly. A written document will, for example, tell staff what to do in case of unexpected turnover. Preparing written internal controls will clearly communicate specific responsibilities to individual staff, facilitate training new staff, and enable you to review and monitor your internal control system. This internal control plan should be developed by professional and managerial staff and must be formally approved by the department head. The department plan must be readily available upon request to auditors.

In addition to a documented internal control plan, agencies should ensure that other essential types of documentation are maintained. Documentation is any paper or electronic information which provides evidence about all aspects of a transaction (who performed the transaction, who approved it, what action was taken, etc.). It provides a financial record of each event or activity, and therefore ensures the accuracy and completeness of transactions. This includes expenses, revenues, inventories, personnel and other types of transactions. Proper documentation provides evidence of what has transpired as well as provides information for researching discrepancies.

Best Practices:

- Prepare an internal control plan for your agency. See the PDF entitled “Preparing an Internal Control Plan” for more information.

- Well-designed documents help ensure the proper recording of transactions. Consistent use of standard forms or templates should be considered whenever possible.

- Comply with the applicable record retention policy set by your department or agency. Ensure documents are kept no longer than the retention period. For a list of RI agency specific retention schedules, see the website of the RI Secretary of State.

Segregation of Duties

Segregation of duties is a primary principle in any internal control plan. The principle of segregation of duties is especially important when using computers and other information technology, because it ensures the separation of different functions such as data compilation, input, and review. It also defines authority and responsibility over transactions and use of the State's resources.

Segregation of duties is the means by which no one person has sole control over the lifespan of a transaction. The fundamental premise of this concept is that an individual or small group of individuals should not be in a position to initiate, approve, undertake, and review the same action. These are called **incompatible duties** when performed by the same individual. The separation of duties assures that mistakes, intentional or unintentional, cannot be made without being discovered by another person.

The list below offers some examples of incompatible duties:

- Managing operations of an activity and record keeping for the same activity
- Custody of assets and recording receipt of those assets
- Authorization of transactions and custody or disposal of the related assets or records.

Different personnel should perform the different functions of data entry, authorization, custody, and report review. If this control activity is properly planned, implemented, and adhered to, departments can safeguard state funds.

Segregation of duties may vary depending on each department's size and structure. Maintaining segregation of duties is especially challenging for units with small numbers of employees. Managers of such departments must consider this principle when designing and defining job duties and they must implement control procedures to assure segregation of duties exists. In an environment with limited numbers of clerical and administrative personnel, management needs to be involved in documenting, reviewing, and approving transactions, reports, and reconciliations.

A department internal control plan, however, should ensure that all of the following activities, at a minimum, are properly separated. The internal control plan should clearly define, assign and document the segregation of duties put in place. The segregation of duties should be able to be demonstrated to an outside party.

Best Practices:

Personnel & Payroll Activities

- Individuals responsible for hiring, terminating and approving promotions should not prepare payroll or personnel transactions or input data.
- Payroll managers should review and approve payroll deductions. Supervisors should review time sheets before approving either by written or electronic signature, but should not be involved in preparing payroll transactions.

Other Expenditure Activities

- Individuals responsible for data entry of encumbrances and payment vouchers should not be responsible for preparing or approving these documents.
- A department should not delegate expenditure transaction approval to the immediate supervisor of data entry staff or to data entry personnel. Individuals responsible for acknowledging the receipt of goods or services should not also be responsible for purchasing or payment activities.

Inventories

- Individuals responsible for monitoring inventories should not have the authority to authorize withdrawals of items maintained in inventory.
- Individuals performing physical inventory counts should not be involved in maintaining inventory records

Check Writing Activities

- Persons preparing checks should not be signing the checks.
- Persons signing the checks should not be reconciling the checking account.

Revenue Activities

- Individuals receiving cash into the office should not be involved in authorizing bank deposits.
- Individuals receiving revenue or making deposits should not be involved in reconciling the bank accounts.

Control Access to Assets and Resources

Internal control systems should involve procedures to restrict access to and enhance control over resources. Resources include money, equipment, supplies, inventory, and the records that account for these assets. Maintaining accountability for the use and custody of resources involves assigning specific responsibilities to specific individuals. Managers should monitor expenditures, revenue collection, and physical assets to ensure that these resources are used only to achieve specific and identified purposes. For example, passwords and identification codes limit access to computer data. Require that passwords and identification codes be kept confidential. Hardware should also be protected. Monitor and control access to cash, equipment, and supplies.

Best Practices:

Department Head Signature Authorization

A department head is responsible for all activities conducted by the department. Because in most departments the department head cannot personally review and certify all business transactions, the department head is responsible for setting up the department’s business operations with a series of checks and balances (internal controls) to balance risks and efficiencies.

- Ensure that department heads directly authorize individuals within their chain of command to be their designee for approval of fiscal documents or other legal obligations on their behalf. There can be no sub-delegation by designees.

Administrative Organization

- Keep an up-to-date organizational chart that defines the reporting relationships as well as responsibilities, including back-up responsibilities, regarding internal controls within the unit.
- Document such processes as opening and distributing mail, administration of keys, access to documents and other administrative controls.

Security of Records

- Ensure the security of records and sensitive information provided or available. The security of records and data in hard copy or electronic format involves system security, data security and physical security.
- Threats to security may come from within, as well as from the outside of an agency so consideration for each is needed.

System Security

- Determine each employee's security access level. Management can limit access to one or more specific business area, i.e. accounts payable, payroll, etc.
- Within each business area, select the appropriate security and approval levels.

Data Security

Data security is the means of protecting data, whether in hard media or in computer and communications systems, against unauthorized disclosure, transfer, modifications or destruction whether accidental or intentional. Therefore, data security helps to ensure privacy and protect confidential data concerning employees, vendors, and the public.

Data security consists of procedures that prevent unauthorized access to computer resources. Appropriate security procedures should not significantly hinder a person from performing their work. Security procedures should, however, protect data from unintentional acts, as well as intentional ones. Examples of data security include:

- Define carefully the level of system access an employee is given
- Select appropriate password safeguards
- A hard to guess password
- Periodic password changes
- Alphanumeric characters per password
- Password kept confidential
- Screen-saver passwords
- Assign each user a unique user ID
- Limit user access to system software
- Control access to specific applications and data files

- Limit access to what is required to perform a person’s job function and to allow for appropriate segregation of duties
- Review security logs
- Limit concurrent logins
- Activate intruder detection and prevention mechanisms
- Implement adequate virus protection procedures

Access to enterprise systems should be reviewed quarterly, as well as when significant turnover occurs in sensitive positions or in realignment of duties.

Physical Security

Physical security is the protection of personnel, clients, records, and assets. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism. Security engineering involves three elements of physical security: (1) obstacles to frustrate trivial attackers and delay serious ones, such as locks and swipe card access; (2) detection devices such as alarms, security lighting, and security guards to make it likely that attacks will be noticed; and (3) security response to repel, catch or frustrate attackers when an attack is detected.

Best Practices:

- Limit access to records and assets to those who have been authorized and have a business need for them. Do not allow electronic records to be downloaded to mobile workstations and transported outside the office.
- Keep important records in lockable, fireproof storage.

Employee Turnover

Access to records and assets must be limited to those who have been authorized and have a business need.

Best Practice:

- Develop a checklist for removing access to records upon separation of an employee or upon transfer out of the unit. Develop a process and assign a point person the responsibility of administering the process for deleting access to records.

Reconciliation

Reconciliation is the process of comparing transactions and activity to supporting documentation. The process ensures the accuracy and validity of financial information and that unauthorized changes have not occurred to transactions during processing. Further, reconciliation involves resolving any discrepancies that may have been discovered.

Reconciliations are a detective internal control; however they may also serve as a preventative control. For example, if employees know that all bank statements will be reconciled and reviewed, they will be less apt to make an inappropriate payment.

Reconciliation processes are most effective when they are consistent and thorough. Employees involved in the reconciliation process should be knowledgeable and clear on their responsibilities and expectations. It should be clear to an external reviewer when a reconciliation has been completed.

Best Practices:

- Ensure information is reconciled to the appropriate supporting documentation. This assists to ensure that transactions are valid and are correct in purpose. (

- Ensure that transactions have been properly authorized. Especially, if the source documents are paper based, review for potential changes to the document between approval and processing of transactions.

- Document a plan for the research and correction of errors or discrepancies of each type of transaction or activity. Communicate these processes and procedures with the appropriate staff.

- Establish expectations for timeliness of error correction.

Section 6- Information and Communication

The overall objective of the fourth component of internal control is that information is current, accurate, appropriate in content and made available on a timely basis at all staff levels to permit management to achieve its objectives. Management uses quality information to support the internal control system.

As a manager, you must be able to obtain reliable information to determine risks and communicate policies and other information to those who need it. To effectively achieve this objective, here are some helpful tips and guidance to keep in mind:

- Your agency's internal controls should outline the specific authority and responsibility of individual employees. These controls can also serve as a reference for employees seeking guidance on handling unusual situations.

- The internal control plan should provide for information to be communicated both within the organization (up as well as down) and externally to those outside, for example, vendors, recipients, and other departments.

- Management should process relevant data into information and maintain quality throughout the processing.

- This communication section of the internal control plan should require that:
    i. Supervisors communicate duties and responsibilities to their staff
    ii. Staff and middle management alert upper management to potential problems
    iii. Administrative and program staff communicate requirements and expectations to each other and
    iv. Separate communication lines are in place such as whistle blower hotlines to enable anonymous or confidential communication when normal channels are inoperative or ineffective

- Select appropriate methods of communication. Managers should distribute copies of the department's internal control plan to all staff whose jobs are affected in any way by the information in the plan. Sending information electronically allows for new procedures and other information to immediately be distributed to a large staff.

- When making changes to internal controls, discuss the changes with the affected managers and staff to determine if the changes will accomplish the control objective. In evaluating possible alternatives, consider the costs and expected benefits of implementing control objectives in a cost-effective manner.

- Prepare and distribute the results of the evaluation and any related changes.

- Conduct in-house training sessions upon releasing new or extensively revised internal control plans to explain the meaning of the plan and the importance of internal controls. This training should also be part of the orientation of new employees.

- Schedule regular staff meetings. These meetings allow you the opportunity to hear your staff's opinion on the overall progress of the agency. Staff meetings provide participants a means to share ideas on how to plan ahead and also discuss weaknesses within their area.

- Select the appropriate method of communication to external parties. When doing so, management should consider the audience, the nature of information, availability, cost, and legal or regulatory requirements.

Section 7 – How to Monitor Effectively

Since internal control is a dynamic process that has to be adapted continuously to the risks and changes an organization faces, monitoring of the internal control system is essential to help ensure that internal control remains aligned with changing objectives, environment, laws, resources, and risks. This fifth component of internal control should be implemented after risks are identified, policies and procedures put into place, and information on control activities communicated to staff.

The effectiveness of your agency's controls should be continually monitored. The organization should select, develop, and perform ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. Monitoring is typically conducted through the use of management activities such as:

- Performance evaluations
- Ongoing supervision
- Status reports
- Independent reconciliations.

Ongoing evaluations may include routine operations built into business processes such as continuous monitoring, supervisory reviews, reconciliations, and self-assessments by management. Separate valuations may include periodic evaluation and testing by internal audit and quality assurance reviews of internal audit, audit committee inquiries of internal and external audit.

The organization should evaluate and communicate internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management, as appropriate. When reviewing, consider internal and external changes, personnel turnover, new programs, administrative activities, and priorities. Schedule monitoring on a regular basis or it is likely to be by-passed by the emergencies of day to day work. Testing controls at least annually allows you to determine whether the controls continue to be adequate and are still functioning as intended. Auditors, program monitors, and other reviewers can be a resource in monitoring internal controls.

Always follow up to ensure that any identified problems are corrected. Management should ensure identified internal control deficiencies are remediated on a timely basis. Further, management should complete and document corrective actions to remediate the deficiencies.

Section 8 – Preparing an Internal Control Plan

An internal control plan is a description of how an agency expects to meet its various goals and objectives by using policies and procedures to minimize risk. In preparing the plan, refer to the five components. Evaluating current internal controls is the first step toward preparing an internal control plan, therefore use the information acquired throughout the evaluation to prepare the plan. Internal control plans can take many different forms, depending on the organizational structure and business practices of the organization. In general, however, the internal control plan should:

- Discuss the goals and objectives of your agency/department
- Briefly state the integrity and ethical values expected of all staff, and especially, the ethical values top management expects of itself (control environment)
- Describe the risks to meeting goals and objectives and
- Explain how the structure, policies, and procedures of the organization act to control the risk (control activities).

In a small agency, the plan might include all the department's policies and procedures. In a large department, the plan might incorporate the various policy and procedure documents by reference. As an integral part of the department's plan, however, these policies and procedures need to be reviewed and updated at least annually. Finally, the internal control plan should also include a section describing to whom the plan is distributed and another section describing how the plan is to be monitored.

State managers have an obligation to administer and safeguard the resources that are entrusted to their care. State managers are accountable not only to their immediate supervisor, but also to the legislature who appropriated the funds, program constituents, fellow state employees, and lastly to the taxpayers who provide the resources that the state uses. An internal control plan helps managers meet this vital responsibility.

Internal Control Guide & Resources

Section 9 – Works Cited

The following research was used in composing this Internal Control Guide:

"Control Environment and Organizational Structure." *The National Association of State Auditors, Comptrollers, and Treasurers*. NASACT, 29 Sept. 2011. 09 Jan. 2014. <http://www.nasact.org/nasc/committees/multistate/.../Control%20Environment.doc>.

"Internal Control Guide for Managers." *Office of the Comptroller*. Commonwealth of Massachusetts. 20 Dec. 2013. < http://www.mass.gov/osc/docs/business-functions/bf-int-cntrls/icgsec1.pdf>.

"Internal Control Toolkit." The University of Texas Health Science Center at San Antonio, 2002. Web. 27 Dec. 2013. <http://uthscsa.edu/internalaudit/PDF/ICToolkit.pdf>.

"Internal Controls." *Financial Accounting*. Finance & Facilities, University of Washington, 27 June 2012. 03 Jan. 2014. <http://f2.washington.edu/fm/fa/internal-controls>.

Ramos, Michael. "Evaluate the Control Environment." *Journal of Accountancy*. AICPA, May 2004. 06 Jan. 2014. <http://www.journalofaccountancy.com/Issues/2004/May/EvaluateTheControlEnvironment.htm>.

"Standards for Internal Control in the Federal Government- 2013 Exposure Draft." *United States Government Accountability Office.* Comptroller General of the United States. <http://www.gao.gov/assets/660/657383.pdf>.