Internal Control Guide & Resources

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 approving transactions should have firsthand knowledge of the transactions, 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 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 Section 8 “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. You must require that passwords and identification codes be kept confidential. Hardware should also be protected. Access to cash, equipment, and supplies must be monitored and controlled.

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.