

National Energy and Utility Conference

2010 Conference

June 14-16, 2010
San Antonio, Texas

Session 5C : Program Integrity

Internal Controls and Fraud Prevention

Presented by: Eva B. Pratt
V/P Administration/ CFO
Capital Area Legal Services Corporation

5-C

INTERNAL CONTROLS

Internal Controls is a series of procedures designed to promote and protect sound management practices, both general and financial.

A sound system of internal controls is an important element of risk management. Internal Controls should be an integral part of any organization's financial and business policies and procedures. Internal controls consist of all the measures taken by the organization for the purpose of:

1. Protecting its resources against waste, fraud and inefficiency.
2. Ensuring accuracy and reliability in accounting and operating data.
3. Securing compliance with the policies of the organization.
4. Elevating the level of performance in all organizational units of the organization.

Internal Controls are simply good business practices. Everyone within the organization has some role in internal controls. The role varies depending upon the level of responsibility and the nature of involvement by the individual.

Internal controls can provide only reasonable assurance – not absolute assurance – regarding the achievement of an organization's objectives. Most acts of employee dishonesty start out small and grow over time. Usually it's the trusted employee who commits the act.

With a system of internal controls, the risk could be minimized. No system of checks and balances must ensure that no financial transaction is handled by only one person from beginning to end.

Why are consistent internal controls important?

1. Management decisions, financial reports, and company taxes rely on the accuracy of figures recorded.
2. Gives the owner control of dollars in and out.
3. Standardized good management practices and procedures.

Advantage of improved internal controls

1. Can reveal errors and omissions.
2. Protect Assets
3. Discourage employee theft.

The first step in developing an effective internal control system is to identify those areas where abuse or errors are likely to occur. Areas such as cash receipts, cash disbursements, petty cash, payroll, fixed assets, grants, and check issuance and deposits.

Internal Controls include:

1. Separation of Duties

Separation of duties is one of the most important control issues that should be addressed in every organization. Certain accounting/bookkeeping functions are designed to cross-reference each other for accuracy. If the same person is responsible for multiple duties, the natural check and balance of the system is destroyed. Trust is not the issue, verifying your business transaction is. Giving a single person unquestioned authority of your finances is not a wise business practice.

In many offices, it is often not practical to maintain a strict division of duties due to a limited staff size. If this is the case, a rotation of duties among personnel with more strict supervision, special double-checking of work and more frequent internal audits could help to assure reliable internal control.

Checklist:

- a. Is the person who handles your cash also responsible for recording cash?
- b. Does the person who pays or orders inventory also receive the material?
- c. Are two or more people responsible for the accounting function?
- d. Is only one person responsible for reviewing financial statements each month?
5. Is your review of financial journals sporadic?

If you answered yes to any of these questions, you have a potential problem.

2. Bank Reconciliations

Reconcile accounts within 10 days of receiving the bank statement. Bank statements can only flag discrepancies if they are reconciled on a timely basis. Reconciliations should be done once a month. Bank adjustments need to be tracked carefully from one month to the next. Bank staff makes mistakes as well as your staff.

Segregation of duties is also important in this area. Reconciliations should be performed by one person and reviewed by another. In a small organization, the executive director should review the bank statements. Also, the person who writes the checks should not have the authority to sign checks.

Checklist:

- a. Do you compare payroll checks with your current employee records?
- b. Do you review canceled checks and endorsements on a monthly basis?
- c. Do you questions funds transferred between bank accounts?
- d. Do you verify reconciled items? (reconcile to the general ledger, not just the amount in the checkbook)
- e. Does the Executive Director receive and open bank statements prior to turning them over to be reconciled?
- f. Do you track the number of credit card bills you sign each month?

If you answered no to any of these questions, you have a potential problem.

3. Physical Safeguards

Access to checks or petty cash is limited, secured and documented when used. **Never write a check out to Cash for any reason.** Petty cash checks should be made out to a person using either “Mary Jones, Agent for the organization or “Betty Smith, Petty Cashier.”

Use two separate bank accounts for your organization. One should be the main account used for deposits. The second should be a subsidiary account that all checks are written against (zero balance account). Checkbooks and blank checks should be kept in a safe and not in a file cabinet.

If you require two signatures on checks, but have trouble getting both signatures when checks need to be signed, have the board change the policy to one signatory for checks up to a specific dollar amount. There is increase risk when one signer signs blank checks because he/she will be unavailable to sign the checks on the date they are processed. (Have auditor make recommendation to the board).

Check signers should never sign blank checks. Nor should they sign checks without any supporting documentation or original supporting documentation.

Use a payroll service and encourage all employees to have direct deposit. This way you don't have to chase down that second signature. Many banks offer free checking accounts for people who use direct deposits.

Limit advances and reimbursements to staff for supplies. Set up accounts with the stores that the organization uses most often and limit your purchases to where there are accounts. Remove employees from the list of authorized users as soon as they are no longer employed with your organization. Verify your list of authorized purchasers on a regular basis.

Review your receivables monthly. Send out second or third notices, if necessary. If you have a finance department of one, train other staff to make deposits. Deposits should be made daily or as often as checks/cash are received.

Checklist:

- a. Are blank check stock and signature stamps safely secured?
- b. Do you restrictively endorse all checks when received?
- c. Do you maintain a list of office furniture, equipment and company vehicles?
- d. Do you have adequate insurance coverage for assets?
- e. Are all systems backed up on a daily basis and is backup stored off-site?
- f. Is there password restriction and security for all computer systems and programs?
- g. Are passwords changed at least every sixty days?

If you answered no to any of these questions, you have a potential problem?

4. Employee/Personnel

Personnel need to be competent and trustworthy, with clearly established lines of authority and responsibility documented in written job descriptions and procedures manuals. Know your employees and be aware of changes in behavior.

Require individuals in high-risk areas to take mandatory annual vacations of at least two weeks. Job rotation or independent audit of function should be implemented when two week vacation is started. Beware of individuals in sensitive positions who are workaholics: never take vacations or for only a day or two at a time.

Checklist:

- h. Have you noticed a significant change in lifestyle in any of your employees?
- i. Are any of your employees extremely possessive of work records and reluctant to share their tasks?
- j. Do you permit your accounting personnel to work longer than a year without a vacation?
- k. Are any of your employees apprehensive about vacations and time off, while always being the first in the office and being the last to leave?

If you answered yes to any of these questions, you have a potential problem.

These are just a few measures that can perhaps help to eliminate the high risk of fraud in your organization. There are generally three requirements for fraud to occur: 1) motivation, 2) opportunity and 3) personal characteristics. It is difficult to have an effect on an individual's motivation for fraud. Personal characteristics can sometimes be changed through training and awareness programs. Opportunity is the easiest and most effective requirement to address to reduce the probability of fraud. By developing effective systems of internal control, you can remove opportunities to commit fraud.

There is no such thing as a perfect control system. In order to achieve a balance between risk and controls, internal controls should be 1) proactive, 2) value-added, 3) cost effective and 4) should address your exposure to risk.