

# INTERNAL CONTROL

## And Fraud Prevention

BY ROBERT PAZ

Internal control is a process that ensures the things we want to happen will happen, and the things we don't want to happen won't happen. An organization's owners, board of directors, managers and other employees may take these essential controls for granted. In most organizations, upon close examination, poor design or a disregard of established policies and procedures could lead to a high risk of fraud and a high degree of inefficiency.

A well-designed system of internal controls can minimize the risk of fraud, increase the reliability and accuracy of financial reporting, and improve the effectiveness and efficiency of operations.

### **TONE AT THE TOP**

At the center of a well-designed internal control system is the control environment. It begins with "toning at the top," which is directly linked to integrity, ethical values, employee competence and managerial philosophy and operating style. If managers do not enforce policies or consistently

override controls and tolerate incompetence, no system—no matter how well designed—will function effectively.

When designing an internal control system, a contractor must balance the cost of maintaining the system against the costs of potential fraud and inefficiency. The first step in design and maintenance of an internal control system is risk assessment—a process of identifying, evaluating and deciding how to manage events. Risks are identified as internal and external events that threaten the accomplishment of the organization's objectives. Internal

risks include personnel changes, new computer systems and theft of expensive tools or inventory. External risks include economic conditions, regulatory changes and work environments. In conducting a risk assessment, a contractor should answer these three questions:

- What is the likelihood of an event occurring?
- What would be the impact if it occurred?
- What can the company do to prevent or reduce the risk?

Once risks are identified and measured, a contractor can design control activities to mitigate the risks. These control activities occur through the entire organization and often are linked between individuals and departments, depending on the size of the company. Control activities include:

- **Separation of duties.** Divide responsibilities so one individual does not control all aspects of a transaction. This reduces the opportunity for an employee to commit and conceal errors (intentional or unintentional) or commit fraud.
- **Documentation.** Retain adequate documentation for policies and procedures and major transactions.

- **Authorization and approval.** Ensure transactions are approved and executed only by employees acting within the scope of authority granted by management.
- **Security of assets.** Secure and restrict access to equipment, cash and confidential information to reduce the risk of loss or unauthorized use.
- **Reconciliation and review.** Examine transactions, information and events to verify accuracy, completeness, appropriateness and compliance. Ensure frequency is adequate to detect any questionable activities in a timely manner.

Next, a contractor needs an information-gathering and communication system to enable personnel to identify, capture and exchange pertinent information to conduct, manage and control operations. This means selecting an accounting software system to gather and process financial information; ensuring correct and pertinent information is collected and properly input into the system; creating lines of communication; and having appropriate tools to disseminate vital information.

Once the system is designed and functioning, a contractor should monitor the controls to verify it is achieving the

desired results. Monitoring is necessary to react dynamically to changing conditions. Controls cannot be outdated, redundant or obsolete. A contractor also should periodically test compliance with policies and controls.

#### TYPES OF CONTROLS

Controls generally fall into two types. Preventive controls deter unwanted events from occurring, while detective controls uncover a problem before it grows into a big problem.

- Examples of preventive controls are:
- computer passwords to stop unauthorized users;
  - purchase orders with set spending limits to prevent unauthorized purchases;
  - logs to track usage of high-value tools and equipment;
  - segregation of billing and collection functions to prevent unauthorized or fraudulent adjustments to accounts receivable records; and
  - credit limits to minimize potential bad debts.

- Examples of detective controls are:
- cash counts and bank reconciliations;
  - budgets that monitor expenditures

- against budgeted amounts;
- hand delivery of payroll checks to employees;
- bank statements delivered directly to and reviewed in detail by the company owner or another high-ranking individual outside of accounting; and
- a fraud tip hotline.

Internal controls do not start with a strong set of policies and procedures, they start with a strong control environment and appropriate leadership from top managers and owners. Managers, not an accounting firm, ultimately are responsible for a company's internal controls.

Although strong internal controls do not provide absolute assurance that fraud will not occur in an organization, they provide reasonable assurance that the organization's objectives for accuracy, efficiency and reduced risk of fraud are met. The entire organization must be responsible for following all policies and procedures underlying these internal controls.

---

**Robert Paz is director of construction industry services at Sax Macy Fromm & Co., PC, Clifton, N.J. For more information, call (973) 472-6250 or email rpaz@smf-cpa.com.**