



CPAs & Business Advisors

17501 East 17th Street, Suite 100 • Tustin, CA 92780-7924 • www.hmwcpcpa.com  
(714) 505-9000 • Fax: (714) 505-9200 • E-Mail: cpas@hmwcpcpa.com

*Member:*  
American Institute of Certified Public Accountants  
Alliance of Merger & Acquisition Advisors  
AHA Affiliated Healthcare Advisors

*Global Representation:*  
INTEGRA  INTERNATIONAL

## **Protecting your company against business fraud**

An adage says “crime doesn’t pay.” But when it comes to fraud, it definitely does pay to prevent it. In fact, a 2002 study by the Association of Certified Fraud Examiners (ACFE) reports that U.S. businesses lost \$600 billion because of fraud in 2001.

One of the best ways to prevent fraud is to develop solid internal controls. But there is no such thing as a one-size-fits-all control. When creating procedures, it’s imperative that you weigh the cost of implementing and maintaining controls vs. the cost benefit of having the controls in place.

### **Balancing procedures**

In examining your internal controls, keep in perspective what you’re trying to protect.

For example, there would be little benefit to creating elaborate procedures to ensure that small office supply items are removed from work areas daily and stored overnight in a locked closet. On the other hand, there would be tremendous benefit to a company to implement control procedures that restrict access to research and development data.

Although no two companies will have the same controls, here are some general guidelines and tips to creating a set of controls:

**Develop a fraud policy.** Your policy must spell out the actions your company will take if an employee commits fraud. To ensure that all employees understand the policy, distribute a copy during employee training and follow up with a discussion period.

The policy’s purpose is to create a climate that is hostile to fraud. To do this, assess how you identify risks in the organization and what action you can take to mitigate the risks. In addition, review what type of system you’ll use to evaluate and monitor controls.

***Perform background checks.*** Background checks on potential employees, suppliers and customers are vital to reducing fraud. Conduct periodic financial checks on employees who handle assets, such as inventory, or proprietary information, such as trade secrets. Remember, even trusted employees can commit fraud if they’re experiencing severe financial problems.

**Segregate duties.** This action provides checks and balances over assets. For this reason, it’s important that an employee who serves as a custodian of an asset not be responsible for the authorization and record keeping of the asset.

The segregation of duties applies to functions as well. For example, the purchasing function should be independent of the disbursement and accounting function.



CPAs & Business Advisors

17501 East 17th Street, Suite 100 • Tustin, CA 92780-7924 • www.hmccpa.com  
(714) 505-9000 • Fax: (714) 505-9200 • E-Mail: cpas@hmccpa.com

Member:  
American Institute of Certified Public Accountants  
Alliance of Merger & Acquisition Advisors  
AHA Affiliated Healthcare Advisors

Global Representation:  
INTEGRA  INTERNATIONAL

**Require approvals.** Require both requesting department manager and accounting department approvals to pay an invoice. The manager approves the expense while the accounting department verifies the math on the invoice.

**Monitor assets.** This can be done in a number of ways including using security cameras and conducting surprise audits or checks. For example, periodically perform a random check to ensure employees in the storage or receiving areas have proper authorization.

It's also important to restrict access to assets. This can be accomplished through security guards, checkpoints, fences, gates, locks and badges. You also can restrict usage of assets, such as computers, with passwords.

### **Detecting fraud**

While the above procedures are largely designed to prevent fraud, there are measures you can take if you suspect that fraud has occurred.

Just as computer programs are used to analyze weather systems or complex genetic codes, auditors can use computer programs to analyze data that appears on documents that are frequent targets of fraud, such as vendor invoices, customer purchase orders and employee expense accounts.

The computer program not only analyzes key information on each document, it also cross-checks the data with information from other databases. The program searches for suspicious information or unusual patterns.

Common tests an auditor performs include:

- Determining if the vendor has a post office box instead of a street address,
- Cross-checking employee data to determine if the vendor address matches an employee's address,
- Checking for unknown or unauthorized vendors,
- Examining the vendor's invoice numbers to see if there are duplicates, and
- Searching for sequentially numbered invoices that are spread over a long time period.

After the auditor performs the tests, the program generates an exception report. Even though the computer has provided the red flags on vendor invoices, it's still necessary to follow up and investigate the information to determine if the invoice is from a legitimate vendor and for goods and services actually received or performed.

### **Supporting fraud protection**

A good fraud policy will go a long way toward discouraging unethical behavior and ensuring that management's decisions are properly carried out. And like any business process, fraud prevention needs the support of high-level management to succeed.