



QuickBooks® 2009  
Overview of Internal Controls

## Overview of Internal Controls for Companies Using QuickBooks®

A White Paper by Stephen King  
President & CEO of GrowthForce

If you are an owner of a small business, your greatest business risk may also be one of your most valued employees – your office manager. This is the employee who often keeps the books, runs the payroll, tracks the inventory and is most likely to “rip off” the company.

Based on a study by the Association of Certified Fraud Examiners, nearly two-thirds of fraud crimes are committed by the business’ employees – with only 12 percent having a prior criminal record. Approximately 42 percent of all cases occur in small, privately-held companies. On average it takes a company 18 months to discover a theft from within its ranks with the median loss being \$132,000<sup>1</sup>.

That is bad news for any business and is why no system should be built on trust. Instituting a system of internal controls that prevents fraud is critical for all small businesses. An ideal system of internal controls has four components:

- **Control Environment:** Create an organizational tone which supports internal controls
- **Risk Assessment:** View risks relevant to the company’s objectives
- **Control Activities:** Recommend internal policies and procedures
- **Communication:** Communicate a clear set of internal policies and procedures
- **Monitoring:** Assess and change internal controls periodically

---

<sup>1</sup>Association of Certified Fraud Examiners

## Internal Control System Benefits

According to a September 2008 report by the CPA Journal, companies that have an bookkeeping system with internal controls have a competitive advantage. During a crisis, they can respond quicker to a risk event, turning it into opportunity. They are able to provide financial information on a timely and accurate basis within the correct accounting period. Correspondingly, management has sufficient knowledge to make the best financial decisions for the company.

## Common Types of Fraud

The most common methods of fraud which occur in businesses with one hundred or less employees can be avoided with proper controls. Intuit, the makers of QuickBooks, has introduced several new features which are designed to deter incidents of internal theft.

Here are four scenarios of employee fraud that all small business should guard against. These scenarios are exclusively for business owners and their CPAs. If placed in the wrong hands, these tricks could be equivalent to dropping the key to the safe in someone's pocket.

### Check Tampering

Check tampering is an expensive problem resulting in a median loss of \$140,000 (1). Electronic check writing has made tampering even easier.

Here is how it works: An employee who prepares the checks makes one payable to himself, signs and cashes the check, then changes the payee field on the electronic check to a legitimate vendor. It looks like Sprint cost \$500 a month but your employee took home an extra \$6000 a year, tax free.

There are several control measures to detect check tampering. The owner or manager should open the bank statement (manually or electronically) and review the cancelled checks. This should never be delegated to the employee doing the data entry. In addition, the bank reconciliation should not be performed by the employee responsible for entering data into QuickBooks. That gives them the keys to the safe. The bank reconciliation is where the errors should be caught and they are, in effect, policing themselves...

If you don't have enough staff, outsource the bank reconciliation process. If your CPA doesn't provide this service, GrowthForce would be happy too. Whoever does the bank

reconciliation should check the payee on the check equals the payee in QuickBooks. This separation of duties is the key to strong internal controls

Another great control measure is to utilize a new technology called SmartVault which allows you to scan documents and attaches them directly to QuickBooks transactions for instant online access anytime, anywhere. For example, SmartVault allows businesses to attach an invoice to a check in QuickBooks. This validates the payment. It is a smart way to store and share documents as well as a secure and easy-to-use solution that integrates seamlessly with QuickBooks. For more information check out [www.smartvault.com](http://www.smartvault.com) or email [info@growthforce.com](mailto:info@growthforce.com)

The **QuickBooks Audit Trail Report** can also be used to identify fraud by scanning the report for a changed payee entry. You can filter that report by transaction type, user, etc – making it a very effective audit control tool. Starting in 2006 the QuickBooks audit trail can not be disabled –which means all transactions are recorded in history making it easier to discourage check abuse.

A more complicated, but successful anti-tampering control, is reviewing a company's **budget versus actual reports**. Many small businesses do not go to the trouble of preparing a budget. They feel it is too time consuming and not accurate. But predicting the future by definition is not accurate. So when a business starts budgeting, they should just make a **SWAG** (serious wild ass guess). By the end four quarters of actual numbers, they will have a good handle on forecasting the future and seeing variances versus actual. This helps flag variances against expected spending.

### Skimming

Skimming is when an employee steals funds received as payment from a customer. To conceal the theft, the employee creates a bad debt or credit memo and applies it to the customer's account receivable balance.

To avoid this scenario, which results in the median loss of \$70,000 (1) per business, separation of duties is recommended. Separation of duties is recommended to avoid this scenario, which results in the median loss of \$70,000 (1) per business. A supervisor or outsourced firm should be designated to review the account receivable credits or write-offs.

The QuickBooks Enterprise Solutions (“QBES”) edition has built in controls which can lock down QuickBooks at screen level. You can limit users by screen or bank account and give them access to view, print, edit, delete and change transactions – or any combination thereof. An employee can now be denied access to A/R credit memos or transaction deletion in Quickbooks. Don’t let employees who billing also have access to delete invoices or create credit memos. That allows them to conceal their own deceit.

One flaw in QuickBooks should be noted. If an employee is in the same session and has not logged out, he can delete his own transactions even if he has no deletion rights. Those deletions will still show up on the audit report, however, so if you review the audit trail report, you’ll catch them in the act. Make it part of your month-end closing process and you’ll sleep better at night.

### Lapping

Lapping involves the employee theft of a cash receipt followed by the application of a future cash receipt from a different customer against the first customer’s receivable. The best way to prevent lapping is to have proper segregation of duties between personnel. The employee receiving checks should have no access to the recording of the accounts receivable records. QBES can now be set to allow or deny employees user rights access.

### Changing prior periods

Another major fraud scenario is employee theft of inventory. To hide the theft, the employee adjusts the QuickBooks inventory to match the physical one. That requires an inventory adjustment which would be caught on the financial statements. So the employee writes off the adjustment to a prior financial period that no one will ever review because the tax return has been completed.

To stop this scam, QuickBooks now has the ability to “close a prior period.” This feature, under Edit, Preferences, Accountant allows you to create a separate “closing” password. This feature restricts the ability to change past periods to a designated user such as the owner, manager or CPA. You can’t edit a prior period transaction unless you have the password. There is also a new feature called Closed Period Transactions under Accountants Report which can detect changes to past periods. We strongly recommend your CPA or

accounting service close the prior period so your bookkeeping staff can't hide transactions in the past. They'll have to reverse them to make sure retained earnings do not take a hit but that's not hard to do.

### Payroll Fraud

Payroll fraud is one of the most costly schemes. The median loss to a business from payroll manipulations is \$140,000 (1). Here is one way it is done. An employee with rights to edit year-to-date payroll changes the withholdings to an amount higher than that actually withheld. The company then pays the difference through a payroll tax deposit and the employee claims a higher tax refund. If a bi-weekly employee adds just \$500 per period in withholding taxes paid to the IRS, that amounts to close to a \$10,000 bonus in a year!

What can a business do to impede this kind of self-inflicted raise? In QBES user rights can be restricted for editing payroll transactions. When reconciling individual employee federal withholding taxes, management can take the "reasonableness test" by asking the question: "Does this sound reasonable knowing this employee's pay?" In the long run, the best practice may be to simply use a third party payroll provider or Professional Employment Organization (PEO) who will require an owner or managers' approval on payroll changes.

### Small Business Internal Control Challenges

When it comes to instituting internal controls, there are three typical areas where small businesses stumble: separation of duties, defining policies and procedures, and managing information systems.

#### Lack of separation of duties

To properly separate duties, a business needs three different employees: 1. someone to authorize transactions 2. Someone to record them 3. To keep custody of the related assets. If sufficient staff is not available to accomplish this tri-fecta, an accountant or third party can provide checks and balances.

If outsourcing is not feasible, other compensating control methods can be implemented such as detailed budgets, exception reports and after-the-fact transaction reviews by managers. For example, the warehouse manager can be asked to assess the monthly inventory adjustment reports prepared by the bookkeeper – putting two sets of eyes on the transactions.

## Inadequately documented policies and procedures

When it comes to internal controls, failing to properly document policies and procedures is the biggest weakness facing small businesses. Often businesses run on an ancient wisdom called “tribal knowledge.” When a member of tribe leaves, so does the knowledge.

Recording policies and procedures insures that management direction is still carried out when an employee leaves. Without documentation, it is difficult to train new employees resulting in higher clerical error rates, incorrect financial statements and more need for supervision.

In response, GrowthForce has developed a series of templates for policies and procedures manuals. These documents are created using **Mirek’s MWSnap** freeware which cuts and pastes screenshots into the manuals. A best practice is to then post the procedures on a Wiki such as **Brainkeeper.net** for easy access to searchable procedures. For CPA firms, creating procedure manuals can be a profitable, value-added service that gives piece of mind to their clients.

## Insufficient control over QuickBooks applications

Managing information technology systems is not a core competency of most small businesses. As a result, they typically fail in three IT areas:

- Regulating authorized users of accounting data
- Controlling deletions and alterations to information
- Making financial data available when needed

Establishing appropriate user names and passwords is critical to accomplishing an adequate system of internal controls. Owners and office managers should have separate user names to provide an audit trail. All Quickbooks users need a separate username. If anyone logs on with the “administrator” user name, there is a weakness of internal controls.

Restricting the use of unauthorized third party systems is critical now that QuickBooks can access and integrate with other systems like point of sale (POS). While these downloads are designed to save time, they can also cause data entry nightmares if incorrectly posted for 365 days by an inexperienced, unauthorized user.

Controlling deletions and alterations is easier with new QBES password and user ID requirements. QuickBooks can be set up to require that passwords be changed every 90 days. Credit card or payroll access requires “strong” passwords due to new government regulations such as HIPPA. With hackers running the dictionary to find passwords, alpha-numeric passwords are not strong enough anymore. Using exclamation marks and asterisks in passwords is recommended.

## Summary

No system of internal controls can completely eliminate fraud, however most employee fraud is a preventable and un-necessary expense. Business owners should be aware of the most common types of fraud and implement best practices to avoid them. In response to the fraud problem, Intuit has updated the QuickBooks Enterprise edition with numerous tools designed to put internal controls in place. Outsourcing is another top choice of many small businesses which do not want to worry about fraud, training and turnover in their accounting function.



For More Information  
Please email [info@growthforce.com](mailto:info@growthforce.com) or call 281-358-2007.

GrowthForce would be happy to review your current use of QuickBooks processes and make recommendations or provide outsourced services to help you improve your internal controls and reduce the risk of fraud.