

Intuit[®]*Academy*

Internal Controls for
Small Businesses to
Reduce the Risk of Fraud

intuit[®]

Copyright

Copyright 2009 Intuit, Inc.
All rights reserved.

Intuit, Inc.
5601 Headquarters Drive
Plano, TX 75024

Trademarks

Intuit, the Intuit logo, QuickBooks, QuickBooks Pro, Quicken, TurboTax, ProSeries, Lacerte, and QuickZoom, among others, are registered trademarks and/or registered service marks of Intuit, Inc. or one of its subsidiaries in the United States and other countries. Other parties' trademarks or service marks are the property of their respective owners and should be treated as such.

Notice To Readers

The publications distributed by Intuit, Inc. are intended to assist accounting professionals in their practices by providing current and accurate information. However, no assurance is given that the information is comprehensive in its coverage or that it is suitable in dealing with a client's particular situation. Accordingly, the information provided should not be relied upon as a substitute for independent research. Intuit, Inc. does not render any accounting, legal, or other professional advice nor does it have any responsibility for updating or revising any information presented herein. Intuit, Inc. cannot warrant that the material contained herein will continue to be accurate nor that it is completely free of errors when published. Readers should verify statements before relying on them.

About the Author



Michelle L. Long, CPA, MBA
Owner, M. Long Consulting, LLC
Author of: ***Successful QuickBooks Consulting***
Lee's Summit, Missouri
www.MLongConsulting.com
www.SuccessfulQuickBooksConsulting.com

Michelle L. Long, CPA is an Advanced Certified QuickBooks ProAdvisor, a national trainer for Intuit presenting the fall 'What's New' seminars and represents Intuit at various conferences throughout the United States. She is one of the elite few members of the Intuit Trainer/Writer Network—Tier 3 and is also a consultant with Intuit Product Development. She has written and recorded numerous courses for Intuit Academy. Michelle is the author of the book *Successful QuickBooks Consulting: The Comprehensive Guide to Starting and Growing a QuickBooks Consulting Business* and was the Technical Editor for Laura Madeira's book: *QuickBooks 2009 Solutions Guide*. She is a Certified QuickBooks Enterprise ProAdvisor, Certified QuickBooks POS ProAdvisor, and Sleeter Group Certified Consultant.

Michelle is the owner of M. Long Consulting, LLC, which provides QuickBooks consulting and training, CFO advisory services, and coaching to growing businesses and entrepreneurs. She is an Adjunct Professor of Strategic Management at University of Missouri—Kansas City and formerly as an Adjunct Professor of Entrepreneurship at Johnson County Community College, she taught FastTrac Business Planning and Entrepreneurial Marketing.

Michelle was named a Financial Services Champion of the Year for 2007 by the Small Business Administration in recognition of her dedication to helping entrepreneurs and small business owners.

Michelle is a Certified FastTrac Facilitator and has facilitated the Ewing Marion Kauffman Foundation's FastTrac NewVenture program and Listening to Your Business workshop. She has been instrumental in helping hundreds of entrepreneurs start and grow their business.

Before starting her own consulting practice, Michelle worked with Price Waterhouse and Hallmark Cards, Inc. She earned a Bachelor of Science in Accountancy from University of Missouri-Columbia, and an MBA in Entrepreneurship from University of Missouri—Kansas City.

CONTENTS

About the Author	3
Introduction	5
Overview of Fraud Statistics	7
Why Should a Small Business Care About Internal Controls?.....	10
Overview of Key Components for Good Internal Controls	11
Tone at the Top—Management.....	11
Accounting System Procedures and Controls	13
Financial Statement Accuracy and Fraud Prevention	14
Internal Controls	15
Segregation of Duties—Policies and Procedures	15
Red Flags for Fraud.....	20
Review and Oversight.....	22
How to Implement Internal Controls in QuickBooks	25
Restricting Access to the Application and Data Files—User Names and Passwords	25
QuickBooks Enterprise Solutions	30
Always-on Audit Trail Controls	33
Voided/Deleted Transactions Report.....	36
Previous Reconciliation Reports.....	37
Controlling Transactions in Closed Periods.....	38
Using Reports to Detect Billing Scheme Frauds	41
Using Reports to Monitor Bad Debt Write-offs	42
Budgetary Controls	43
Customer Credit Card Protection	44
Understanding Key Preferences.....	45
QuickBooks: Online Banking and Bill Pay	51
Effective Backup Procedures	54

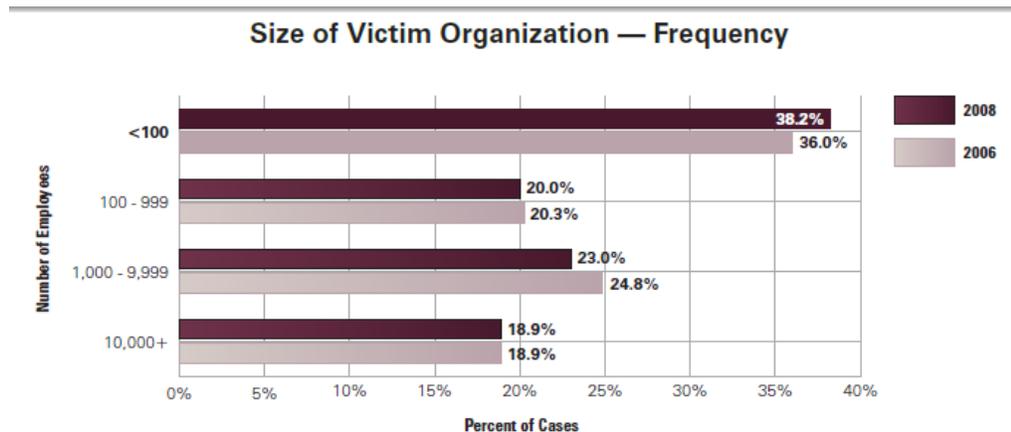
Introduction

Fraud is a bigger problem than you think. Most growing businesses have to fend off many different kinds of threats: competition, economic changes, and the rising costs of goods or human resources—the list can be long. But one large threat to businesses can be a silent, looming killer—fraud.

Fraud comes in a variety of forms, including credit card and check fraud as well as employee theft. Some of the most common types of employee fraud include stealing assets either directly or through fraudulent billing schemes or check tampering. Some specific examples include: paying fictitious vendors, skimming cash, claiming undue overtime, stealing inventory, or embellishing an expense account.

Regardless of the nature of the fraudulent activity, the propensity for loss is tremendous. Fraud can threaten the stability of a business by resulting in significant financial losses. The Association of Certified Fraud Examiners (ACFE) reports the typical business will lose an average of 7% of revenues from employee theft alone.

Although fraud and corruption can occur in large corporations or small businesses alike, based on the report from the ACFE 2008 Report to the Nation on Occupational Fraud & Abuse, “small businesses—defined as those with less than 100 employees—suffered both a greater percentage of frauds (38%) and a higher median loss (\$200,000) than their larger counterparts. These findings accentuate the unique problems in combating fraud—primarily the limited amount of fiscal and human resources available for anti-fraud efforts—frequently faced by small organizations.” The ACFE Report includes the following graphs to illustrate:¹



¹ 2008 Report to the Nation on Occupational Fraud & Abuse, by the Association of Certified Fraud Examiners, www.acfe.com.

Size of Victim Organization — Median Loss



The ACFE Report contains a lot of useful and interesting information. This course references only a few charts and graphs, whereas the full report is much more comprehensive with statistics by industry, type and size of organization and more. For more details visit the ACFE website at www.acfe.com.

In this course, we will give an overview of a few fraud statistics as they relate to small businesses, explore internal controls and how small businesses can benefit from putting these controls in place, and finally discuss red flags which might indicate fraud. This course is an overview and does not include every possible scenario or control which may be possible. The intent is to provide suggestions which are feasible for small businesses with limited staff and resources to help deter or reduce the risk of fraud. As the business grows, their internal control procedures should as well.

As accounting professionals, we are the trusted advisor for our clients. We owe it to them to educate them about the risks of fraud, the importance of good internal controls and how to implement them. This course includes suggestions for how to overcome the lack of segregation of duties that is often present in small businesses due to the lack of staff, and discusses the important role the business owner and outside accountant can play in helping to create a good internal control environment. Red flags which may be indications of fraud will be discussed along with numerous reports which are helpful in reviewing and monitoring the financial records.

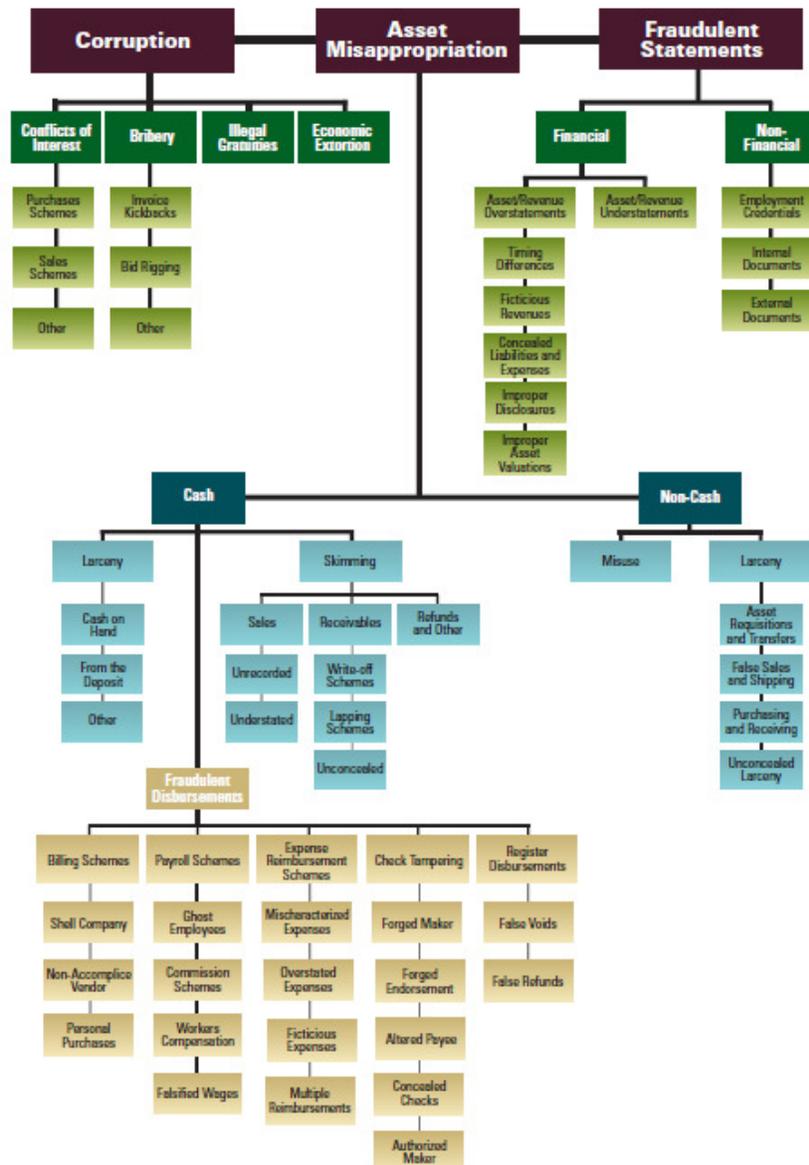
Overview of Fraud Statistics

The ACFE's 2008 Report to the Nation on Occupational Fraud and Abuse has classified fraud into three categories—corruption, asset misappropriation and fraudulent statements defined as follows:

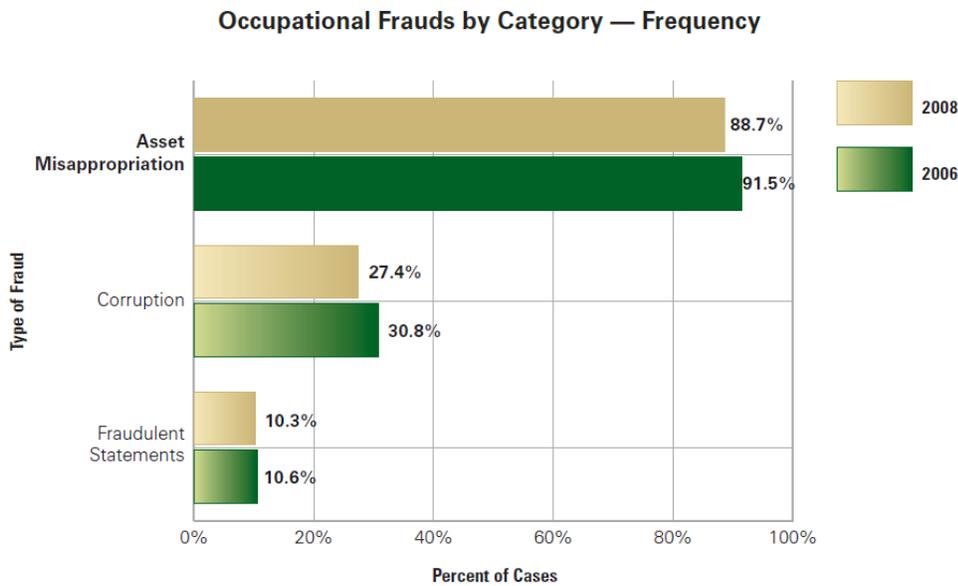
Asset misappropriations schemes are frauds in which the perpetrator steals or misuses an organization's resources.

Corruption refers to schemes in which fraudsters use their influence in business transactions in a way that violates their duty to their employers in order to obtain a benefit for themselves or someone else.

Financial statement fraud involves the intentional misstatement or omission of material information from the organization's financial reports; these are the cases of 'cooking the books' that often make front page headlines.



The ACFE report further defines the frequency of fraud based on these three broad categories in this chart:



Within the broad category of asset misappropriation, it is helpful to understand exactly which types of fraud are most common in small organizations (as shown in the chart below from the ACFE Report). Internal controls should be implemented to deter or reduce the risk of these schemes and management should be aware of these to be alert to potential red flags.

Small Businesses — <100 Employees (342 Cases)		
Scheme	Cases	Percent
Billing	98	28.7%
Check Tampering	87	25.4%
Corruption	79	23.1%
Skimming	71	20.8%
Expense Reimbursement	53	15.5%
Cash on Hand	53	15.5%
Cash Larceny	52	15.2%
Non-cash	51	14.9%
Payroll	48	14.0%
Fraudulent Financial Statements	42	12.3%
Register Disbursements	12	3.5%

The ACFE's report also provides descriptions of the categories of asset misappropriation along with the median loss by category:

Asset Misappropriation Sub-Categories					
Category	Description	Examples	Cases Reported	Percent of all cases ²	Median Loss
Schemes Involving Cash Receipts					
Skimming	Any scheme in which cash is stolen from an organization before it is recorded on the organization's books and records.	<ul style="list-style-type: none"> Employee accepts payment from a customer but does not record the sale 	159	16.6%	\$80,000
Cash Larceny	Any scheme in which cash receipts are stolen from an organization after they been recorded on the organization's books and records.	<ul style="list-style-type: none"> Employee steals cash and checks from daily receipts before they can be deposited in the bank 	99	10.3%	\$75,000
Schemes Involving Fraudulent Disbursements of Cash					
Billing	Any scheme in which a person causes his or her employer to issue a payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases.	<ul style="list-style-type: none"> Employee creates a shell company and bills employer for nonexistent services Employee purchases personal items, submits invoice to employer for payment 	229	23.9%	\$100,000
Check Tampering	Any scheme in which a person steals his or her employer's funds by forging or altering a check on one of the organization's bank accounts, or steals a check the organization has legitimately issued to another payee.	<ul style="list-style-type: none"> Employee steals blank company checks, makes them out to himself or an accomplice Employee steals outgoing check to a vendor, deposits it into his own bank account 	141	14.7%	\$138,000
Expense Reimbursements	Any scheme in which an employee makes a claim for reimbursement of fictitious or inflated business expenses.	<ul style="list-style-type: none"> Employee files fraudulent expense report, claiming personal travel, nonexistent meals, etc. 	127	13.2%	\$25,000
Payroll	Any scheme in which an employee causes his or her employer to issue a payment by making false claims for compensation.	<ul style="list-style-type: none"> Employee claims overtime for hours not worked Employee adds ghost employees to the payroll 	89	9.3%	\$49,000
Cash Register Disbursements	Any scheme in which an employee makes false entries on a cash register to conceal the fraudulent removal of cash.	<ul style="list-style-type: none"> Employee fraudulently voids a sale on his cash register and steals the cash 	27	2.8%	\$25,000
Cash on Hand Misappropriations	Any scheme in which the perpetrator misappropriates cash kept on hand at the victim organization's premises.	<ul style="list-style-type: none"> Employee steals cash from a company vault 	121	12.6%	\$35,000
Non-Cash Misappropriations	Any scheme in which an employee steals or misuses non-cash assets of the victim organization.	<ul style="list-style-type: none"> Employee steals inventory from a warehouse or storeroom Employee steals or misuses confidential customer financial information 	156	16.3%	\$100,000

²The sum of percentages in this table exceeds 100 percent because several cases involved multiple asset misappropriation schemes from more than one category.

It is clear that asset misappropriation presents the greatest risk (but not the only risk) for small businesses. It is also clear that the most frequent methods of fraud for small businesses surround cash received and cash disbursements. Although, theft of inventory and payroll can and do occur, they are less frequent than schemes surrounding cash.

Why Should a Small Business Care About Internal Controls?

Obviously, small businesses should care about internal controls to protect their assets and reduce the risk of fraud. Additionally, the growing awareness of fraud has caused investors and other companies to focus on stronger internal controls at the smaller, private companies. Not that they have to spend millions or even thousands of dollars to implement internal controls – they shouldn't – they don't have that regulatory requirement. But, understanding internal controls and how they can protect themselves and their small business is important.

Many small businesses are finding that banks or other financial institutions want to see stronger evidence of internal controls in the companies that they lend money to, and even from their audit firms.

Reasons a small business may want to create strong internal controls:

- Strong internal controls focus on getting the financial statements right – working on internal controls now will address and prevent future or potential problems
- An outside party such as an investor, banker or accountant recommendation
- To solve present business problems and/or help prevent fraud from occurring
- The potential to go public
- Working with a Sarbanes-Oxley (SOX) compliant customer may require it

Good internal controls are essential no matter how small the company, for many valid reasons. Fraud prevention, embezzlement detection, and accurate financials are all reasons to follow good internal control practices. Implementing controls into the financial accounting software alone isn't enough to ensure compliance; it takes some people power too. Since most small business owners have very little accounting background, accountants are necessary to play a key advisory role in helping a business design and implement sound internal controls. Many private companies are seeing benefits from implementing internal control provisions relating to accountability, independent audits, internal controls and document retention.

Overview of Key Components for Good Internal Controls

There are several factors necessary for creating good internal controls to reduce the risk of fraud:

- Tone at the top—management
- Accounting system—segregation of duties, policies and procedures
- Financial statement accuracy, compliance and review

Tone at the Top—Management

Management's commitment to implementing internal control and how well they follow their own internal controls sends a strong signal to all employees about the importance of internal controls, fraud prevention and financial statement accuracy. In small businesses often management consists only of the business owner and possibly one or two managers. Usually the owner and these managers' background and primary business focus are in their business and not in accounting. Often small business owners undervalue the importance of sound financial information and take a hand-off approach to the bookkeeping. We have even heard of small business owners tell their bookkeeper "You are in charge of the books – I don't want to know the details unless there is a problem." This attitude is present in most fraud cases perpetrated against small businesses.

As accounting professionals, we need to emphasize to our clients (the small business owner) that they must not be too trustful of their employees or bookkeeper nor too busy to spend time to monitor their financials on a regular basis. That is one of the best ways to reduce the risk of fraud—management involvement and oversight.

By taking several simple steps management can reduce the risk of fraud and create a culture that produces accurate and timely financial information.

Take an Interest in the Books

The first and single most important thing a small business owner can do is take an interest in the books. They should ask for and review financial reports on a periodic and random basis. They should have an idea of what these reports should look like and set a range for acceptable thresholds. They should review any significant variances and understand what drives these variances.

This presents an opportunity for accountants to help their clients. These business owners need training and help in learning to generate and read these reports. They also need to understand the importance of the information they are getting and how it impacts the day to day operations of their business. An accountant is the ideal person to help the business owner understand their financials.

Provide Oversight and Review

The second way management fosters a culture of control is by showing the employees they are checking up on them. If an employee sees that they are left to do things with little or no oversight the opportunity to commit fraud will soon present itself. It is important to stress that given the opportunity and the need; sometimes even the best employee will commit fraud. Small business owners often are victims of fraud for the sole reason that they did not understand this.

When talking with owners who have experienced fraud they will almost always tell you that it was someone they trusted; unfortunately it is often a family member or a trusted friend. In most of these situations the employee was seldom, if ever, checked up on or asked to provide documentation. In one

circumstance, a small family restaurant determined that they could not be at the establishment the entire time that they were open so they hired a trusted night manager. After a short period of time, this manager began skimming off of each night's deposits. In hindsight this could have been easily prevented or caught much sooner if the owners had compared nightly deposits to prior period deposits (establishes normal, reasonable thresholds), having one person receiving the cash and another person making the deposit to the bank (segregation of duties), and reconciling the register sales to the actual cash deposited each night (audit of sales receipts versus amounts deposited to ensure agreement between the two). In this case the fact that the manager knew his deposits were not being reviewed presented an opportunity to commit fraud.

Written Ethics Policy

The third item that management should strongly consider is setting up a written policy that clearly outlines a policy for integrity and ethics. Management should make sure that this policy is well known throughout the company. It is imperative that management sets a strong example by modeling the behavior that is expected from their employees. If the boss is seen violating the ethics policies it quickly sends the signal that they are not important. The boss should not take cash out of the drawer, take inventory or office supplies for personal use, mail personal mail with the postage machine or anything else—employees then justify their actions based on the fact that the boss does it, so it is ok for them to do the same thing.

Business owners should consider reviewing and possibly revising their policies on at least an annual basis to adjust for changes in the working environment. Other ways to promote the policy may include posting the policy in a prominent place in the workplace and reviewing the policy with employees during staff meetings or annual interviews. Feedback from employees should be encouraged and can often help owners see things that they might miss when they are not present. Employees can also be asked to sign the ethics policy saying that they will uphold and abide by the terms of the policy. These signed ethics policy statements should be filed in an employee's personnel or HR file.

Random Spot Checking

The final step in management involvement is to change it up. Although there are some items such as monthly financial reports that should definitely be reviewed on a consistent basis; management should also choose other reports and backup documentation to spot check. They want to make sure that an employee can never predict what they will be looking at. An employee intending to commit fraud will try to find a predictable pattern and then exploit it. If they know someone is looking at documentation on a regular basis, it makes it harder for them to implement a fraudulent scheme.

Accounting System Procedures and Controls

One important step in setting up internal controls is creating accounting procedures and implementing controls. This section provides an overview of considerations whereas later sections provide complete details.

One consideration is determining who has access QuickBooks and which areas and functions they will be able to access. In a small business environment the bookkeeping or accounting is often staffed with only one or two employees. However, it is still important to give serious consideration to the areas of the system they are allowed to access. QuickBooks will allow you to limit or even deny a user's access to certain areas of the system. Management should take the time to become familiar with the capabilities of QuickBooks and to limit an employee's access in areas that might be appropriate. As the accounting professional, you can help management implement users and restrict access.

If the client has the benefit of a larger accounting staff, they should limit access by areas of responsibility among staff. For example you wouldn't want someone with Accounts Payable access to be able to balance the bank statement, or to access Accounts Receivables. Individuals who enter and process transactions should not be given rights to set up books or configure organizational settings. No single person in the organization (other than the owner) should have ADMIN rights to everything.

It is important to note, however that this is not the norm in the small business environment. The business owner generally tends to think that since they are not the one with the accounting background; they should be set-up as a user, and the bookkeeper should be the one who is setup as the administrator. This situation allows the bookkeeper access to all critical parts of the information system and the ability to change anything – possibly without detection. You can still set a user up with full rights to all areas (not recommended, but could be OK if additional checks and balances are present as we have been discussing), but not make them an Administrator. The issue with making someone an administrator is that often it allows them to cover their own tracks, or over-ride important control provisions, (like turning off the audit trail when they want to perpetrate a fraud).

Complete details of setting up users and access in QuickBooks are provided later in the course.

Backups of the Data File

Another important consideration to ensure accurate and complete financial reporting is establishing a policy for archival and backup of the financial accounting database. Management should determine how often backups should be made and then create a formal backup policy. Too often in the small business environment the only time backups are made is when the information needs to be given to a third party. There is no single rule for how often a backup should be made. Backups should be made based on transaction volume. Management should consider what amount of data would be too painful to re-create and then backup as often as they would not be willing to re-enter the data. In a business where the bookkeeper comes in once per week and nothing is really done in between, weekly would be sufficient, however if the bookkeeper enters a great amount of detail each day an hourly or twice-daily backup might be appropriate.

Additionally, making backups periodically will retain transactional detail that can then be used to prove fraud, if necessary. For example – if a bookkeeper writes checks on one day, then cashes them and changes the payee the next day, the backup that corresponded to the first day would show the original payee, while the later backup would show the changed payee. So backups stored offsite are not only an important measure in both business continuance and efficiency, but also can add another level of control in preventing fraud.

Effective backup procedures are discussed in more detail later in the course.

Financial Statement Accuracy and Fraud Prevention

Every small business owner should consider having an outside accountant such as their CPA review their books on a periodic basis. Since owners are often not trained in proper accounting procedures and reporting, an outside expert review can be considered not only beneficial but also essential. CPAs can review reports for management purposes without having to issue an opinion and can help management find inaccuracies and inconsistencies in their financial reporting. Just like knowing that management is reviewing their work helps to prevent fraud, knowing that an accountant will be reviewing their work will further help to prevent potential fraud and ensure accurate financial reporting.

A small business owner should review and understand the financial statements even if they are not accountants! Sit down with your clients and help them understand the financial statements. Encourage them to take a seminar on understanding financial statements. Many times the owner does not take the time to understand if his reports are complete or accurate. The small business owner needs to understand that in producing financial documents when signing a tax return or a loan application, there is often an explicit or implied statement that these financial statements are accurate and complete. Business owners should take the time to ensure that they are comfortable with the numbers they are reporting. Also, as a good accounting professional, you can help the business owner understand her financials and ensure that she is comfortable with the numbers she is reporting to the bank or IRS. So this is just another reason to involve a professional accountant in a review of the small business owner's books.

Details about items to review and reports to utilize are provided later in the course manual.

Internal Controls

Internal controls are necessary to reduce the risk of fraud. Without any controls or oversight, it is like leaving the door unlocked with the cash register drawer open hoping that no one will steal any money. Plus, with the additional pressure of a declining economy, the temptation can become too great for some people if there are no controls in place.

Even employees who are honest can be tempted when they see large sums of money right in front of them. This is especially true if the business owner has not implemented any access controls or set up shared control over the business finances.

Also, without internal controls a business owner can never know if their information is complete, accurate or reliable. Time should be taken to set-up, implement and review a policy of internal controls. Once the policy has been established, management should ensure that the controls are being followed. Some of the items to consider in creating an internal control policy are:

- Segregation of duties – policies and procedures
- Safeguarding of assets
- Red flags for fraud
- Review

Segregation of Duties—Policies and Procedures

One of the most important ways to fight—and detect—fraud in a small business is to set up shared responsibilities for the business' financial management. Access to financial assets and information, including the accounting system, should be restricted and carefully controlled. Do not allow this to be a one-person task; make sure there is a separation of duties where no single employee has too much responsibility within the system.

Small businesses can outsource to a bookkeeping firm and/or request quarterly analyses of the financial system by a CPA or other accounting technology expert. Within the company, it is important to divide the financial responsibilities among the management team. For example, they can hire a part-time employee or bookkeeper who is responsible for payroll processing only and perhaps a few other disconnected tasks such as creating invoices or entering bills. This is highly preferable to having one person who manages all aspects of the accounting.

It is easy to have the mentality that with a small office and only one bookkeeper, that segregation of duties is impossible. However, it is important to remember that you don't want one person doing it all. It just takes some time and consideration when setting up segregation of duties.

The first place to start for most small businesses is in controlling the cash. As was discussed in the section covering management review of the books, the owner should never give up check signing responsibility and should review the bank statement and returned checks every month for discrepancies and odd items. (Having the bank statement mailed to the owner's home is a great idea – it prevents anything from being altered after the statement arrives). They then should question the bookkeeper and ask for supporting documentation to support the items in question. This keeps in place key segregation of cash duties. In businesses with two or more accounting staff this means that you have Accounts Receivable separate from Accounts Payable as well.

Cash management is the greatest fraud issue because it is one of the easiest ways to commit fraud. Management should take particular interest in understanding how cash is received, recorded in the books, deposited and then used to pay vendors. The owner should monitor all cash receipts and cash

disbursements to make sure that they make sense. They should look at source documents behind these inflows and outflows. Some simple and practical ways to implement these in a small business include:

Cash Receipts and Accounts Receivable

- When cash comes in the door, the cash or checks should be logged onto a slip for deposit. Sometimes this means you can have the receptionist open the mail, log the checks (make a copy of the log) and give to the bookkeeper to enter in the books. Then, the bookkeeper can make the deposit to the bank. Except in the case of collusion, having two people involved means that they cross check one another and eliminates most cash receipt fraud. The owner should then check the log and compare it against the deposit made.
- Some banks are now offering check scanning capabilities where the checks can be scanned at the office and immediately deposited into the account. The images of the checks can then be maintained electronically. This can also integrate with QuickBooks to automatically record payments received.
- In retail stores, offer customers a cash reward (ie \$5) if they are not given a receipt. This forces the employee to enter the sale into the register and monitor the number of voided transactions.
- All write-offs or credit memos should be approved in writing by Management and filed with the original invoice.

Cash Disbursements and Accounts Payable

- All requests for check or cash disbursements should include a copy of the original invoice or receipt. The invoice should clearly show what is being purchased and the amount. Specify the individual (by title, not name) who is authorized to approve cash or check disbursements.
- Consider having check signing thresholds that require two people to sign the checks in excess of those thresholds. Appropriate threshold depends on company and the amount material to that company.
- Consider the use of purchase orders for purchases over a certain amount. This threshold would vary depending on the size of the business. All purchase orders should be approved and then matched up with any incoming invoices and receipt of the goods and/or services. Invoices without a pre-approved purchase order would not be authorized for payment until reviewed and authorized by management
- Create an approved vendor list. This prevents employees from setting up their friend or relative as a vendor, who then sends in legitimate-looking bills to be paid. Create a policy whereby management must approve a vendor before any business can be done with that vendor.
- Check signors (either one signor or two) should not be the people who are preparing the checks. When reviewing the checks for signing, compare the check amount, payee to supporting documentation - i.e. invoice, purchase orders, item receipt.
- Print out a check register of all checks paid and verify completeness. Make sure that all checks per the register have been reviewed and signed and that there are no additional checks.
- Have someone other than the one who prepared the checks mail the checks. Checks mailed by the same person could get "lost" and "replaced" but perhaps to a different payee than was authorized! This can be accomplished in an easy way by having the check signer also put the checks and the stubs into the vendor envelopes and then seal them for mailing. Then give them to the postman when he comes. This prevents the AP person from changing a check after it has been signed.
- Consider the use of an online bill paying system. If this is used make sure that the business owner is the only one authorized to finalize payment, and that it is password-protected with a password that only the business owner knows.

- Avoid issuing "emergency" checks! If absolutely necessary, create a log for such checks and require receipts being brought back to support the check and review frequently.
- If an employee is sent to a store such as Costco or an office supply store with a blank check to purchase supplies, upon returning the employee should submit a receipt that shows the items purchased and the total tying to the amount of the check. This eliminates the ability of the employee to purchase personal items on this blank check. A common form of fraud involves making small personal purchases in addition to the authorized supplies in amounts that wouldn't raise questions just by the amount of the check and then not turn in the receipt. Over a period of time these purchases can quickly become significant. Better yet – get a company credit card and tie receipts into the statement. Review the statement for completeness. Question missing receipts – if necessary, request a copy from the vendor.
- Employee reimbursements for supplies, travel, meals and other than business expenses should be submitted in a standard format and all receipts should be attached. Management should review and approve all reimbursements before being paid. In addition, a policy regarding reimbursement of travel and meals, etc should be established and all employees required to read and sign it, so as to prevent abuse. It is recommended that employee reimbursements be processed through with payroll.
- If petty cash is used, a petty cash ledger should be maintained and receipts attached for outflows. In QuickBooks, you can set up a Petty cash account as a bank account. When the petty cash fund needs replenished, you enter a check to record the expenditures. Petty cash should be reconciled monthly and the reconciliation and receipts reviewed by management.

Credit (or Debit) Cards

- Require receipts for transactions—do not just download transactions.
- Have separate cards for different users for accountability.
- Reconcile accounts monthly.

Bank Statements/Activity

- The actual bank statements should be sent to the owner's home address. The owner should open and review the bank statements each month.
- The owner should be accessing online accounts to monitor activity on a regular basis.
- If possible, have someone other than the person who writes the checks perform the bank reconciliation. It may be advisable to outsource the monthly reconciliation procedures.

Payroll

This is often a company's biggest expense, so pay attention. It's also a very easy way to commit fraud in a loose, uncontrolled environment. Look for phantom employees, unapproved overtime, extra hours over and above what was expected, unapproved pay raises, loans that somehow do not get paid back, etc.

- Management should know what the expected payroll dollar amounts are, in total. Question anything above that amount immediately. For example, if the normal payroll is \$25,000, and one comes in at \$27,000, question the extra amount immediately. Conversely, if normal payroll is \$25,000 and the hourly employees' workload has been lower than normal, question if that payroll comes in at \$25,000 (it should be lower due to less hours worked).
- Have documentation for any changes to payroll rates...such as a status change form. Ensures changes are made accurately and with authorization. Status form should be signed by the business owner and kept in the employee's permanent HR file, to serve as a documented paper trail.

- Timesheets should be created and approved before payroll is paid. QuickBooks allows you to print Timesheets and they include a signature line for approval. Ideally a supervisor who is familiar with the amount and type of work being performed should be the one to review the timesheets before being sent to the accounting department for processing. If overtime is worked – have the supervisor or business owner sign off on the overtime.
- If reasonable, consider installation of an integrated time clock system. Time theft is one of the most significant forms of employee fraud. The use of a time clock that integrates with the accounting software is one of the best ways to prevent time theft.
- If payroll is outsourced, you still need to be concerned. Pay particular attention to new employees or changes. Have good documentation procedures for how these items are submitted. Watch for phantom employees (usually only an issue in larger companies where an owner may not know the names of each employee.)
- Whether in-house or outsourced review registers and physical checks. Review the register for total employee count, hours worked (no unusual 200 hour workweeks), and salary changes. Many providers will have a changes report. Look at that too and make sure it makes sense.
- Have someone else deliver the checks or use direct deposit.
- Consider using Intuit Online Payroll if you want to keep payroll separate from the QuickBooks financial software.

Inventory

- Ideally, Purchase Orders should be created and matched with Item Receipts. Then, accounts payable should match the bill from the vendor to the Item Receipt prior to approval for payment.
- Documentation should be created and maintained for all requisitions of inventory.
- Inventory should not be taken without proper paperwork. Any inventory taken for samples, donations or discarded due to damage or obsolescence should be properly documented and approved. Then an inventory adjustment should be entered into QuickBooks.
- If employees are allowed to purchase inventory, a form should be created and approved to document when inventory is purchased by the employee.
- Physical inventories should be taken to identify differences between perpetual and physical inventory. Inventory Adjustments should be made as needed to write off obsolete inventory.

Fixed Assets

Many times in a small business, the only list of fixed assets that is maintained is the one prepared by the CPA for tax purposes. Such a relaxed approach to fixed asset management can result in opportunity for theft. Fixed assets represent a significant investment of a company's resources and should be treated that way. If the CPA does maintain a fixed asset list, the owner should get a copy of this list at least annually and keep track of all additions and deletions on a monthly basis. Periodically depending on the size of the company and the value of the assets, a physical inventory of all fixed assets should be taken. Depending on the number and complexity of the assets they may want to consider the use of bar-coding and scanning software to help in the inventory. Once taken any unexpected changes to the list should be researched and addressed. Also important to note – be sure to obtain insurance on all fixed assets in case of fire or theft.

It is advisable for small businesses to maintain their own fixed asset item list in QuickBooks and not just rely on the list maintained for tax purposes. When fixed assets are purchased, they should be recorded on the Fixed Asset Items List in QuickBooks indicating the details of the asset purchased as shown in the screen shot below. This provides improved accountability and monitoring of fixed assets.

Type: Fixed Asset
 Use for property you purchase, track, and may eventually sell. Fixed assets are long-lived assets, such as land, buildings, furniture, equipment, and vehicles.

Asset Name/Number: 2008 Delivery Van - 14
 Asset Account: Trucks

Purchase Information: Purchase Description: 2008 Delivery Van
 Item is: new used
 Date: 10/15/2008
 Cost: 44,500.00
 Vendor/Payee: East Bayshore Auto Mall

Sales Information: Sales Description:
 Item is sold:
 Sales Date:
 Sales Price: 0.00
 Sales Expense: 0.00

Item is inactive:

Fixed Asset Mana...
 Asset Number: 14
 Cost/Basis: 44,500.00
 Year-End Accumulated Depreciation: 31,684.00
 Year-End Book Value: 12,816.00

Asset Information: Asset Description: Propane powered, forest green
 Location:
 PO Number:
 Serial Number: IGMCCCL11W1RB123456
 Warranty Expires: 10/15/2013
 Notes: Full coverage insurance effective 10/15/08.

Buttons: OK, Cancel, Custom Fields, Spelling

Other Various Controls to Safeguard Assets

- Locking doors, registers, offices, file cabinets, blank checks and more
- Restricting access when and where possible
- Passwords and firewalls on computers
- Using security cameras (even fake cameras can deter some criminals)
- Background checks for all employees hired
- Listen to customer/vendor complaints – they could be an indication of a problem

Red Flags for Fraud

Some working situations create an environment where fraud is more likely. Small business owners should be aware of these situations and should try to control the working conditions to try and reduce the opportunity for fraud. These include:

- Inadequate training of employees
- Poor employee compensation
- Unreachable goals or deadlines
- Management's lack of commitment to controls
- Disorganization of work area
- Close association with key employees, customers or vendors
- No attention paid to details
- Little or no review of employees work
- Lack of physical controls inside a company
- Lack of Information System access controls

These situations are not necessarily indications that fraud is being committed, but rather that an opportunity to commit fraud or make material mistakes exists. There are additional warning signs that may be more of a "red flag" that fraud is happening; these include:

- Employee's behavior changes significantly. For example someone who is usually on time begins to be late, a clean person becomes disorganized, or a usually social person withdraws from co-workers.
- An employee begins to take a lot of "personal" calls on their cell phone, and takes these calls out of the office (in the parking lot, or lobby, for example)
- Employee has high personal debt or other financial pressures such as excessive medical bills
- Employee appears to be living a lifestyle that does not fit their current income level
- Excessive use of drugs or alcohol and/or excessive absences due to this use.
- Employee job dissatisfaction
- Significant outside pressures from home or other obligations

We have discussed extensively the fact that management should be reviewing financial information and the importance of doing so. The following items address more specifically what items or types of transactions a business owner may be looking for:

- Irregularities in time – Are there journal entries in the middle of the month that are usually made at month end; entries on Mondays that should be made on Fridays, etc?
- Irregularities in frequency – Do you usually only offer discounts to customers once a month and a review shows they are showing up weekly? Are there too many credit memos? Should deposits be made daily and they are missed a couple of times a month?

- Irregularities in amount – Are the amounts being paid to the office supply store more than they usually are, or is the average daily deposit too low?
- Review balance sheet account balances to determine if they appear to be over or understated
- Transactions are not being entered in a timely manner
- Transactions are being recorded in an incorrect accounting period
- Transactions are being classified to incorrect accounts
- Lack of original documentation for transactions – for example
 - Transactions do not have sufficient documentation or approval
 - Pre-signed checks come back without proper receipts
 - Employee reimbursements are excessive, increasing consistently and don't have adequate supporting documentation
- Missing inventory, office supplies, or physical assets
- Excessive credit memos or adjustments for either Accounts Receivable or (debit memos) Accounts Payable
- Common or insider names on customer or vendor lists
- Duplicate payments or invoices
- Be sure to look for other signs that may be significant for your industry or particular business:
 - An example in the plumbing industry would be a lot of “broken” supplies being booked to jobs – this is usually a sign that plumbing supplies are being bought for a job in excess of what is really needed, then taken home to use on side jobs. The excess and stolen supplies are then booked to the job at work as “broken”. Usually you will see a pattern of who is doing this.
 - An example in the restaurant industry might be a lot of “returns” – this can sometimes indicate employee theft of food.

Review and Oversight

Because the business environment is constantly changing the internal control policies we have discussed should be reviewed for thoroughness and adjustments should be made from time to time.

Changes that may affect the internal control policies may include:

- Increase or decrease in number of accounting staff,
- Changes in accounting staff's training, or personnel.
- Changes in accounting software including upgrades or a new accounting package, and Changes in technology available such as online banking to help with financial processes.

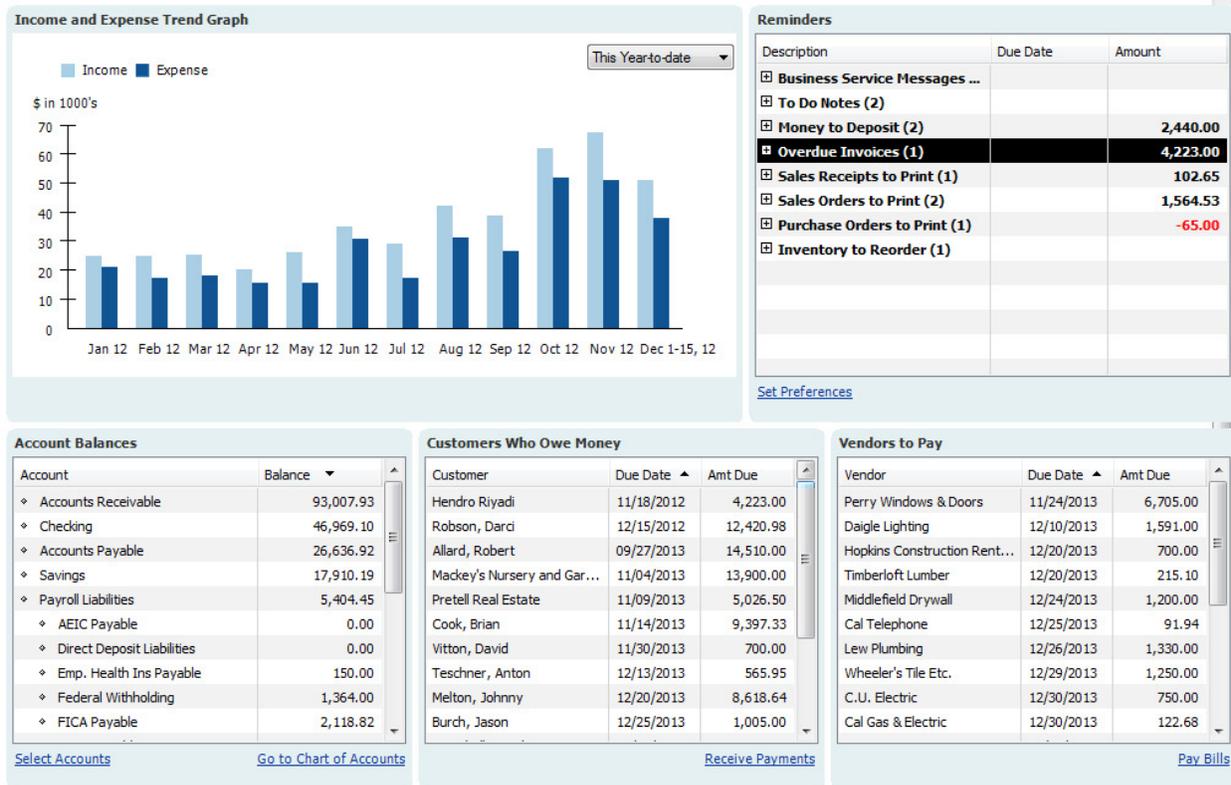
All of these changes and many others that we have not addressed can significantly alter the internal control needs of a company. Many times these changes are positive, but they still need to be addressed and implemented into the internal control policy. At a very minimum, the policy should be reviewed on an annual basis; however it should be reviewed anytime any change to the financial environment of the company would be considered significant.

Suggested Areas of Review Include:

Daily

Deposits – Daily monitoring of cash, check and credit card deposits helps to monitor cash flow and will alert management to changes or fluctuations in deposit amounts. Often in a small business there are not enough personnel to separate the duties of receiving cash and making the deposits. A management review of daily deposits and (if applicable) corresponding daily sales reports will help to offset the risk involved in a lack of segregation of duties over the handling of cash.

Company Snapshot – The Company Snapshot (as shown below) is new for QuickBooks 2009. If the data file is current, it provides a good overview of the status of the company's key financial affairs in one convenient location. The Company Snapshot allows the business owner or management to review account balances, accounts receivable and accounts payable quickly along with an income and expense graph and reminders list.



Weekly or Bi-Weekly:

Check registers and signing of checks – Often clients are tempted to add their bookkeeper as a check signer to their account. They have demands out of the office and want the bookkeeper to be able to keep the bills paid without them having to run back to the office all of the time. This raises the risk of fraud exponentially. One way to keep the control of signing checks and keep things moving smoothly is to consider on-line bill pay service where the owner executes the payment transactions himself.

The staff can enter bills and payments as usual and then management can authorize payment online from any place at any time that is convenient for them. Online bill pay also introduces another level of control for both employees and outside people who may handle checks. Online bill pay also puts the responsibility for the check getting to the intended recipient on the financial institutions you are using and eliminates all chance of employee fraud after the transaction has been sent.

In the case of paper checks that are printed, signed and mailed, these checks should be reviewed after they come back from the bank, as part of the Bank Reconciliation. This will catch a check that has been altered after it was signed.

Accounts Receivable reports – Management should review these reports for collections, billings and write-offs. This will also help to monitor cash flow but will also alert management to other frauds such as unauthorized write-offs. One common form of fraud involves customers paying in cash. If the employee who is receiving the cash also has rights to create credit memos on the customer's account, they can simply create an "authorized" credit and then pocket the cash. A review of all credit memos would prevent this.

Payroll registers – should be reviewed for unauthorized overtime, raises and bonuses. Paychecks should be checked against time cards to make sure that time paid is for actual time worked. Later in the presentation, we're going to talk in detail about good internal controls over payroll.

Monthly

Financial statements – At a minimum the monthly Profit and Loss, Balance Sheet and Statement of cash flows should be reviewed. It may also be beneficial to include percentages and compare these amounts to previous periods

Budget to actual reports – Monthly review of budget variances will help management quickly spot problem areas. It will also help the company in making sound operating and financing decisions.

Bank statements – If the accounting staff is limited and it is difficult to separate key accounting duties managements; review of the bank statement is critical. Ideally the bank statement should be sent to the owner's home or some other address where the owner will be the one to open the statement. Ideally, management (or another employee than the bookkeeper) should be the one to perform the monthly bank reconciliation – if this is not possible, then Management should carefully review and sign off on the completed bank reconciliation every month. Asking spot questions like "what is this entry? Or "What is this bank fee for?" Or – "have we contacted the customer to get this NSF check resolved?" will go a long way in alerting the bookkeeper that Management is watching and adding that additional level of review over the main thing that all businesses care about – CASH. Online banking also allows for the owner to review the statements and easily reconcile the account.

Key reconciliations for AR/AP. Review bad debt details or other write-offs.

Unusual entries to system and all entries greater than a threshold.

Additional reports which may be useful are detailed later in the course.

How to Implement Internal Controls in QuickBooks

QuickBooks is designed to be used by small businesses that need powerful software, but also ease of use and an intuitive interface. Luckily, QuickBooks features very strong internal controls that can be easily implemented by a knowledgeable accountant.

QuickBooks contains strong internal control features that, when properly implemented and used in conjunction with appropriate management oversight, can provide small business owners and managers with reasonable assurance in the accuracy and completeness of their books. It is important to remember however that the software cannot do it alone – management must stay involved in and review the books.

To fully protect confidential business information, there should be strong access restrictions in place. Those access restrictions will protect the business not only from outsiders, but also from employees. If numerous employees use the financial management software, the access restrictions in the software become even more critical. Multi-user environments pose an increased risk of employee fraud or breach of confidentiality.

Restricting Access to the Application and Data Files—User Names and Passwords

The best way to fight employee fraud is by setting appropriate access privileges within QuickBooks Pro, QuickBooks Premier or QuickBooks Enterprise Solutions. This allows you to limit access for specific employees to specific tasks, including payroll processing and reporting. QuickBooks helps you separate access to financial transactions and reports with its user permissions and controls.

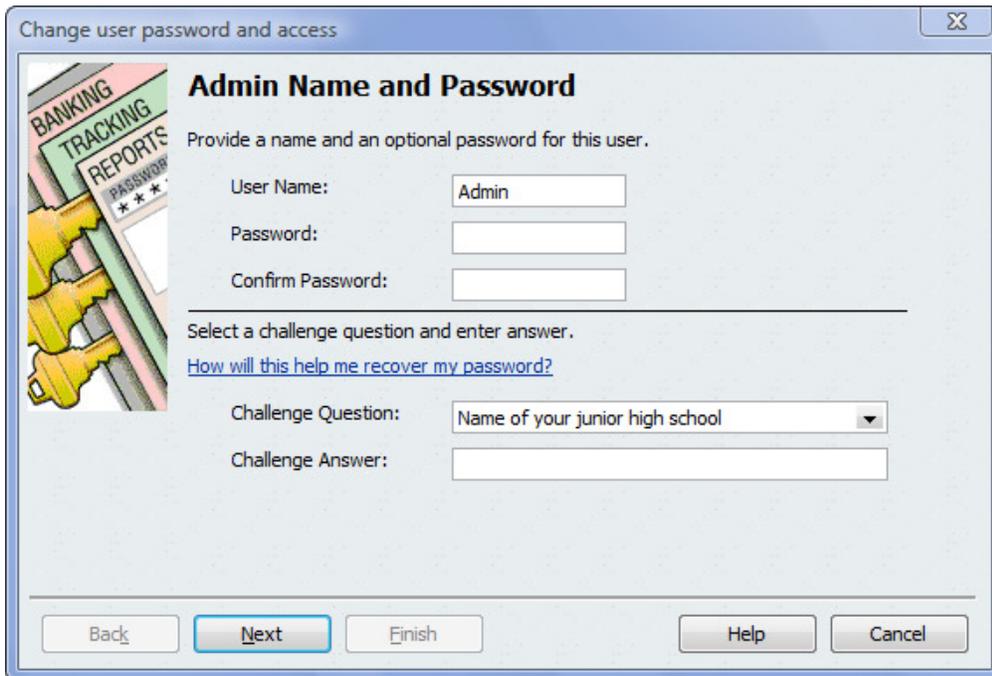
By using this feature, you have the ability to give employees permission to effectively do their jobs, yet still protect sensitive information.

Use these controls to distribute the workload and keep up with growth in the business. You have the control over what you allow people to do in the QuickBooks Company file. Using permissions and roles will not only reduce worry about fraud, but it will also keep employees focused on the areas assigned to them.

Admin User

From the **Company** menu, select **Set Up Users...** If this is the first user to be established for the company, then by default this user will be the QuickBooks Administrator, as shown below.

NOTE: We recommend reserving the Administrator user for the business owner while creating another user for the owner to use on a daily basis. Even though the business owner may not be in the file as often as the bookkeeper, it is important that only the owner have administrator rights to the file. All other users should be set-up with their own user ID and Password, even if you are granting them full rights access. This is because an Administrator user can always over-ride any rights assigned to them and change any company preferences.



The screenshot shows a Windows-style dialog box titled "Change user password and access". Inside, there is a sub-section titled "Admin Name and Password" with the instruction "Provide a name and an optional password for this user." Below this are three input fields: "User Name" (containing "Admin"), "Password", and "Confirm Password". A horizontal line separates this from the "Select a challenge question and enter answer." section. It includes a link "How will this help me recover my password?" and a "Challenge Question" dropdown menu (set to "Name of your junior high school") and a "Challenge Answer" text box. At the bottom, there are five buttons: "Back", "Next", "Finish", "Help", and "Cancel".

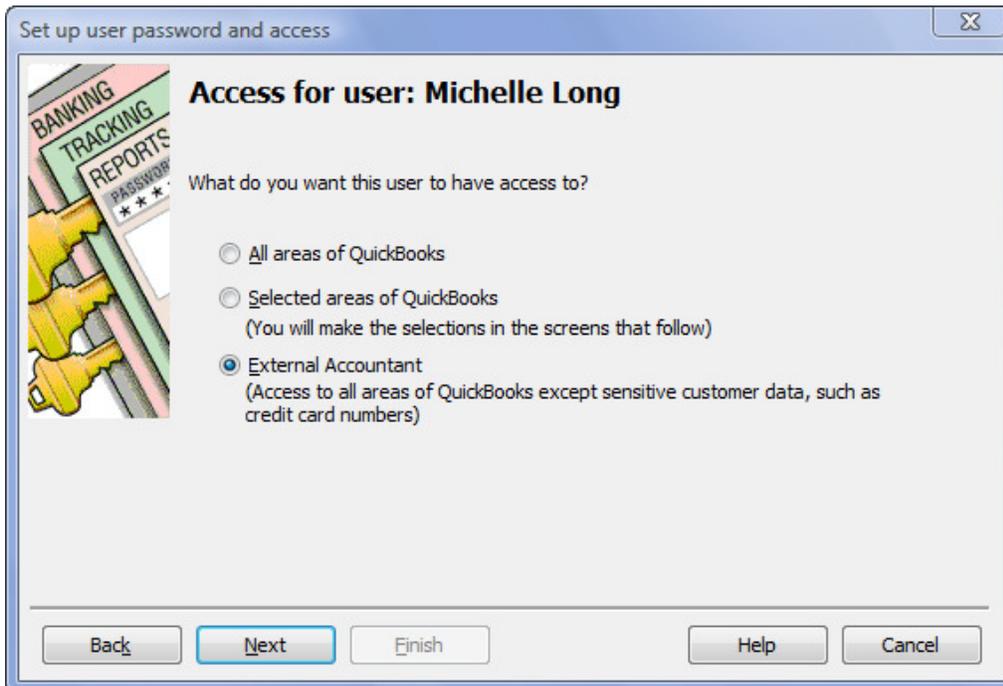
The Administrator has access to *all* areas of QuickBooks; in fact, the Administrator is the *only* user who has access to all areas of QuickBooks and therefore there can only be one user with Administrator rights per company. Accordingly, great care should be taken in determining the individual who will be assigned this User Name. In most cases, the Administrator should be either one of the business owners, the CFO/Controller, or even someone outside of the company such as the company's CPA. In all cases, the User Name of the Administrator should be changed from "Admin" to one clearly reflecting the user – usually the Administrator's first name and last name. (Note: The Admin user should not be used on a regular daily basis as explained later).

Additionally, a strong password should be established for the Administrator; a strong password is generally considered to be one that is at least eight characters in length; contains alpha, numeric, and special characters; is not a word found in a dictionary; etc.

External Accountant

External Accountant is a new type of user. An External Accountant is a powerful user type that can access all areas of QuickBooks except sensitive customer data, such as credit card numbers. If you log in as an External Accountant, you can separate the changes you made during a review from the changes made by your clients, including the administrator.

If you are logged in as an External Accountant user, you can access the Client Data Review feature in the Pro and Premier editions of QuickBooks. Client Data Review is always available in QuickBooks Accountant Edition. If you are performing a review at your client's location, you can use your client's edition of QuickBooks to perform a review, if you are logged on as an External Accountant. This feature is not available if you are logged on as the administrator.

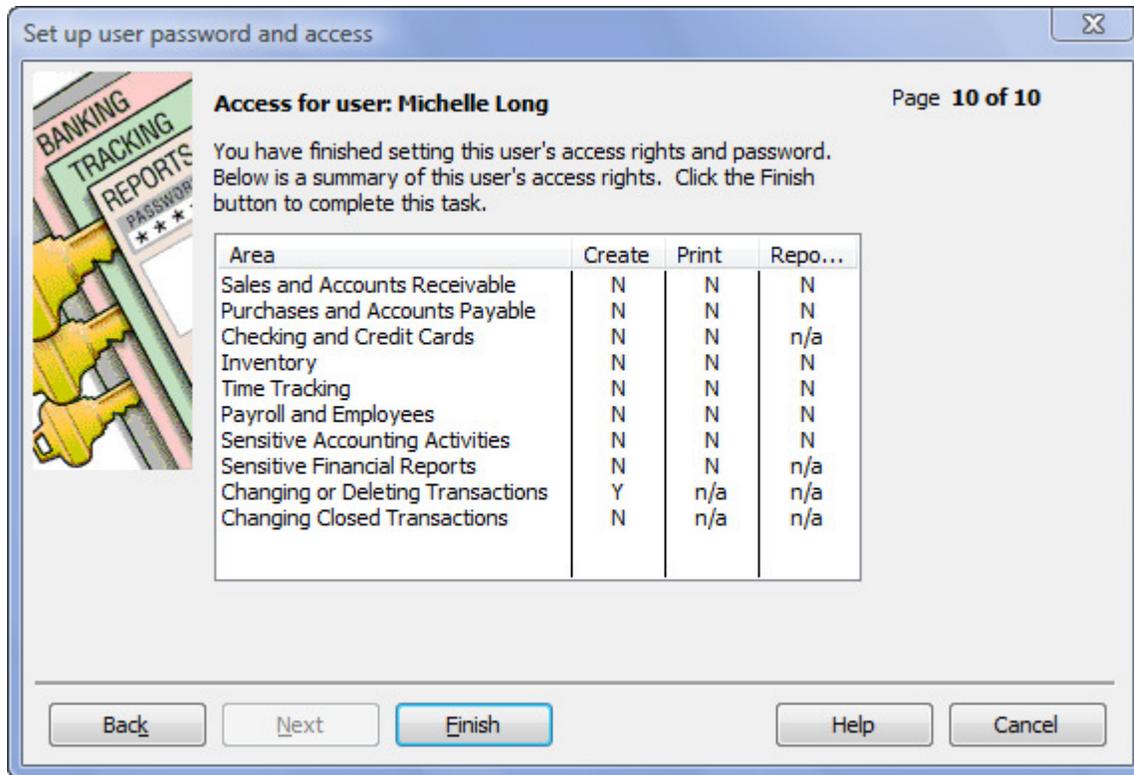


Other Users

Once the Administrator User Name and password have been established, individual User Names and passwords should be established for each and every other user. To initiate this process from the **Company** menu select **Set Up Users** and then click on **Add User** and enter the User Name and password as shown below.

Clicking **Next** opens the screen to Set up user and password (as illustrated previously in the section on External Accountant) which controls what rights may be assigned to this user. In most cases the second option – **Selected areas of QuickBooks** – should be selected so that specific rights may be assigned on an as-needed basis. Depending on a user’s specific job responsibilities, rights may be assigned in up to ten distinct areas:

1. Sales and Accounts Receivable
2. Purchases and Accounts Payable
3. Checking and Credit Cards
4. Inventory
5. Time Tracking
6. Payroll and Employees
7. Sensitive Accounting Activities
8. Sensitive Financial Reports
9. Changing or Deleting Transactions – the answer to this one will vary based on the individual’s level of authority within the company. The safest answer is “no” if you are unsure.
10. Changing Closed Transactions – the answer to this one should in almost all cases be “no” since this will allow a user to change results for prior, closed, periods.



As mentioned previously, some QuickBooks functions can be performed only by the user with Administrator rights. For example, only the Administrator can change Company Preferences, with the exception of the Closing Date and Closing Date Password which can be changed by anyone with Sensitive Accounting Activities rights.

NOTE: As a precaution against accidental changes, it is wise for the user with Administrator rights to maintain a second user profile. This additional profile – without Administrator rights – would be used to log in to QuickBooks to perform everyday tasks. When necessary, the user would log in to QuickBooks with the Administrator profile to perform those tasks requiring Administrator rights; once these tasks are completed, the user returns to the “regular” profile for routine functions.

QuickBooks Enterprise Solutions

QuickBooks Enterprise Solutions offers the ability to have up to 30 users and allows for much greater flexibility and control in setting up the rights and access for these users. Some of these features include:

Advanced User Permissions & Custom Access Levels

Give employees access to the information and activities they need to do their jobs, without exposing the data to accidental or intentional misuse. For example, you can give a user access to use the check register but restrict his access to payroll to prevent him from viewing payroll checks. QuickBooks Enterprise will obfuscate the payroll check entries so he can continue to use the check register without seeing the payroll checks.

- Allow or restrict users to access over 115 individual reports, bank accounts, lists and activities in QuickBooks Enterprise
- Customize each user's access level to
 - View-only
 - Create
 - Modify
 - Delete
 - Print
- View the permissions report (an example is below) to know which users have access to what

Permissions Access by Users

Areas and Activities	Ann Young	Bookkeeper	John Smith
Accounting	None	Full	None
Asset Accounts	None	Full	None
Edit Closed Transactions	None	Full	None
Equity Accounts	None	Full	None
General Journal	None	Full	None
Liability Accounts	None	Full	None
Manage Fixed Assets	None	Full	None
Working Trial Balance	None	Full	None
Banking	Mixed	Mixed	Mixed
Bank Accounts	None	Full	None
Checks	None	View	None
Credit Card Accounts	None	Full	Full
Credit Card Charges	None	View	Full
Deposits	Full	View	None
Loan Manager	None	None	None
Online Banking	None	None	None
Reconcile	None	Full	None
Transfer Funds	None	Full	None
Centers	Mixed	View	Mixed
Customer Center	Full	V-VB	View
Employee Center	View	View	View
Vendor Center	None	View	Full
Company	Mixed	Mixed	Mixed
Billing Solutions Sign Up	None	None	None
Company Information	None	None	None
Company Preferences	None	None	None
Enter Vehicle Mileage	Full	None	None
Find All Transactions	None	Full	None
Planning & Budgeting	None	Mixed	None
Business Planning & Analysis	None	None	None
Set Up Budgets and Forecast	None	Full	None
Print Labels	Full	None	Full
Remote Access	Full	Full	Full
Set Closing Date & Password	None	Full	None
Set Up Online Banking	None	None	None
Synchronize Contacts	Full	None	None
Customers & Receivables	Full	Mixed	Mixed
Accounts Receivable Accounts	Full	Full	None
Assess Finance Charges	Full	None	None
Billable Time and Costs	Full	None	None
Change Item Prices	Full	None	Full
Credit Card Refunds	Full	View	None
Credit Memos	Full	View	None
Estimates	Full	View	None

Predefined User Roles

QuickBooks Enterprise Solutions comes with fifteen (15) predefined roles. These are roles with preset access to areas and activities based on the functions most commonly found in a business. The predefined roles are:

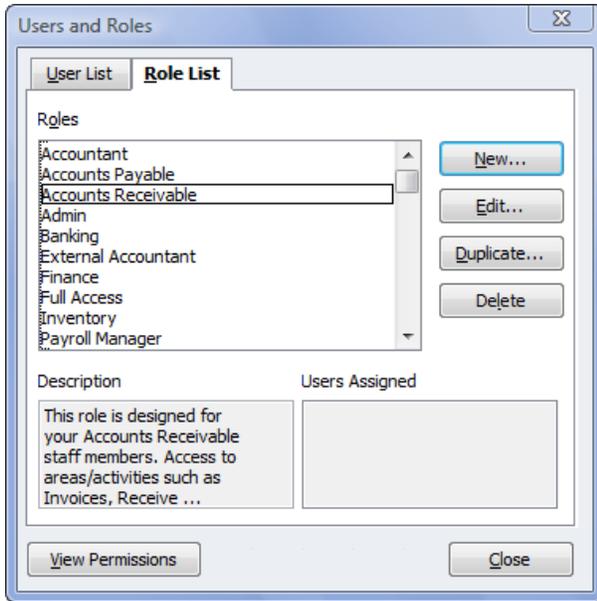
The predefined roles in Enterprise Solutions are:

- Accountant
- Accounts Payable
- Accounts Receivable
- Administrator
- Banking
- External Accountant
- Finance
- Full Access
- Inventory
- Payroll Manager
- Payroll Processor
- Purchasing
- Sales
- Time Tracking
- View-only

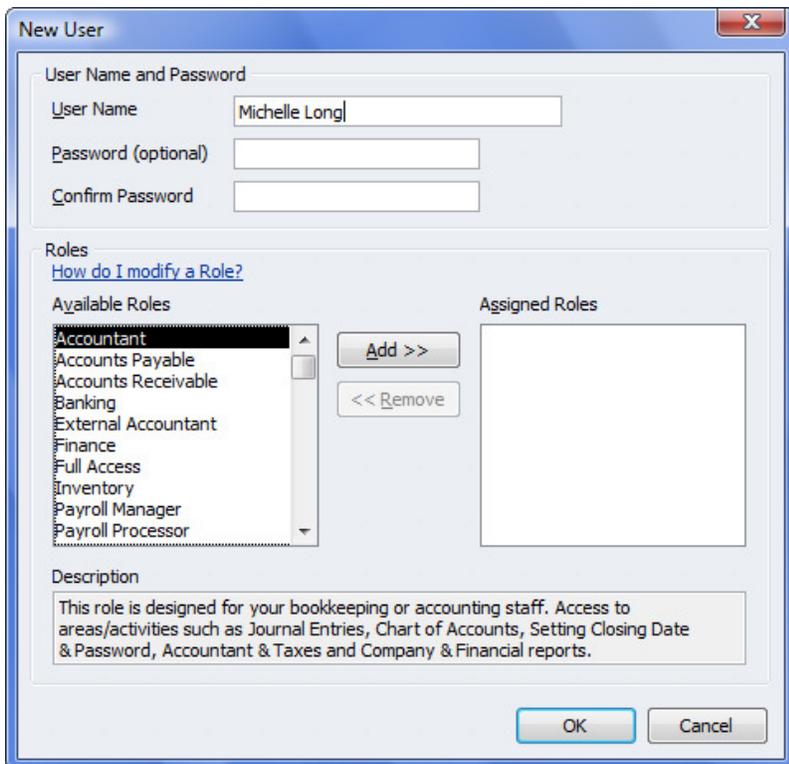
Using roles, you can define a user's permission in extreme detail. For example, in one area the user may have permission to view information, but not create, modify, or delete. In another area, the same role may have permission to view and create but not modify or delete.

To set up good checks and balances, you need to divide responsibilities and tasks. For example, a recommended practice is to have one employee who enters invoices and another employee who enters receipts/credits. You should avoid having the same user process both of these transaction types.

If preferred, the administrator can add new roles to the list. In that case, it is advisable to start by duplicating an existing role. Once the role is duplicated, you can modify the duplicate role to suit your specific needs. Using this approach, you leave the existing roles intact but can save yourself work by borrowing permissions from an existing role.



After you set up roles in Enterprise Solutions, you can create users. When you create a user, you assign a role and a password to the user. You can create, edit, and delete users as necessary. Once your permissions are set up, you can print a very useful report on the permissions granted to each user. Using this report will help you identify modifications you want to make to any given role. The report lists all the areas and activities in QuickBooks Enterprise Solutions for which you can assign permissions, along with a column for each user and that user's permission for each area.



Always-on Audit Trail Controls

One of the most important tools QuickBooks software offers to company owners for internal control is the use of the audit trail. Once individual user profiles have been established in QuickBooks, the effectiveness of the Audit Trail Report as an internal control procedure is increased significantly. The Audit Trail is always on in QuickBooks and the Audit Trail Report provides a summary to the Administrator of all QuickBooks transaction activity answering three essential questions:

1. Who added/edited/deleted the transaction?
2. When was the transaction added/edited/deleted?
3. What were the relevant details of the transaction, i.e., date, amount, accounts, names, etc.?

If there are changes to any of the information in the list below, the change will create an entry in the Audit Trail:

- Transaction date
- Document number
- Payment terms
- Sales rep
- Shipping date
- Modifying user
- Account
- Class
- Associated name
- Amount
- Quantity
- Unit price
- Item
- Payment method
- Due date
- Reconciliation status
- Posting status
- Billed date
- Transaction type
- Line-level discount information

QuickBooks logs all transaction changes in the Audit Trail Report. The Audit Trail Report – shown below – is selected under the Accountant & Taxes section of the Reports menu. Only the Administrator and those users with Sensitive Financial Reports rights can access the Audit Trail Report.

4:21 PM
02/03/09

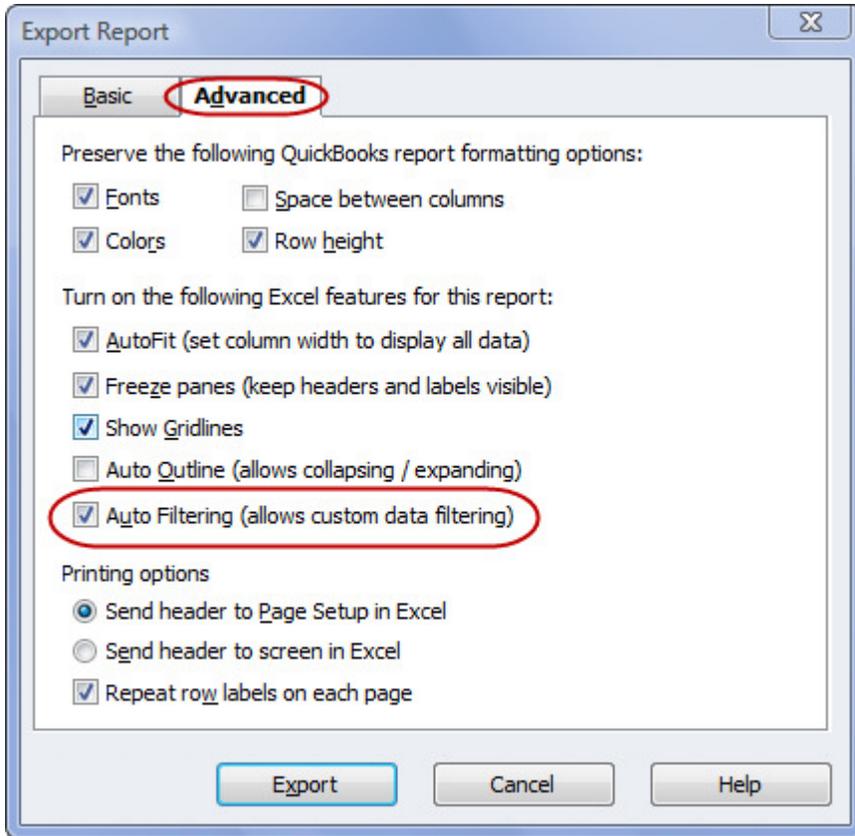
Rock Castle Construction
Audit Trail
Entered/Last Modified February 3, 2009

Num	Entered/Last Modified	Last modified by	State	Date	Name	Memo	Account	Split	Debit	Credit
Transactions entered or modified by Admin										
Check 304										
▶ 304	02/03/2009 16:21:26	Admin	Latest	11/17/2008	A Cheung Limited		Checking	Job Expense...		5,000.00 ◀
					A Cheung Limited		Checking	Job Expenses:Job...	5,000.00	
304	11/17/2008 09:36:22	Admin	Prior	11/17/2008	A Cheung Limited		Checking	Job Expense...		500.00
					A Cheung Limited		Checking	Job Expenses:Job...	500.00	
Deposit										
	02/03/2009 16:21:33	Admin	Latest	11/17/2008		Deposit	Checking	Construction...	350.00	
					A test		Checking	Construction Incom...		350.00
	11/17/2008 09:35:30	Admin	Prior	11/17/2008		Deposit	Checking	Construction...	550.00	
					A test		Checking	Construction Incom...		550.00

As shown above, the Audit Trail Report provides a record of every transaction entered into the data file, including details such as when a transaction is changed and the nature of the change. At a minimum, it is suggested that a business owner or other responsible person examine the Audit Trail Report on at least a weekly basis, looking for any suspicious activity.

- Examples of such activity include unauthorized bad debt write-offs or other credits to customer accounts, journal entries to cash accounts, or changes to the payee on checks.
- Another example of something to watch for might be customer invoices being deleted. This could indicate that an employee received cash from the customer, and then deleted the invoice so he/she could pocket the cash.

At least two potential issues exist with utilizing the Audit Trail Report as a cornerstone of internal control in QuickBooks installations. One is that the report can become quite voluminous and is not easily filtered within QuickBooks to find transactions meeting certain criteria. To effectively resolve this issue, users may export the Audit Trail Report to Excel and, when exporting from QuickBooks, turn on Excel's AutoFilter feature. To do so, open the Audit Trail Report in QuickBooks, click **Export...** at the top of the window and click the **Advanced** tab of the **Export Report** window. Then check the box labeled "AutoFiltering (allows custom data filtering)", as shown below.



Exporting the Audit Trail Report to Excel with AutoFilters enabled adds Excel's drop-down filtering capabilities to the report, allowing it to be filtered easily on virtually every column, as shown below. This allows you to find activity by individual user, by date and more.

	A	B	C	D	E	F	G	H	I	J
1				Num	Entered/Last Modified	Last modified by	State	Date	Name	Memo
2	Transactions entered or modified by Admin									
3		Bill								
4					12/15/2012 11:49:28	Admin	Latest	09/30/2012	Sloan Roofing	Opening Balance as of 10/1/2003 st
5									Abercrombie, Kristy:Remodel Bathroom	Opening Balance
6										
7		Bill 903-01								
8			903-01		12/15/2012 11:49:37	Admin	Latest	10/01/2012	McClain Appliances	
9									Cook, Brian:Kitchen	Refrigerator w/self-clean freezer
10									Cook, Brian:Kitchen	Microwave and double oven combo
11									Cook, Brian:Kitchen	Electric rangetop

Voided/Deleted Transactions Report

QuickBooks also gives you a Voided/Deleted Transactions report. You can use the Voided/Deleted Transactions Report to easily review changes and detect errors. This report is similar to the Audit Trail, but shorter and somewhat easier to use. This is an important report as it deals solely with voided or deleted transactions. This report can help shine a light on devious activity, as deleting a transaction should be a rare occurrence in your accounting system and is a common activity associated with fraud. If you notice that a particular person has deleted multiple transactions, take note and investigate.

For example, here's a real-world fraud case that involved an employee who modified deposits to steal money owed the business:

This particular business provided music and art lessons to students. The employee would accept a customer payment, and then post the payment to the customer account. The employee would then enter a discount on the Receive Payments window offset to some catch-all account such as Opening Balance Equity, an account that has a significant overstated or understated balance for most companies. Cost of Goods Sold and income accounts carry large balances, too, so employees may try to bury activity in the detail of those accounts as well.

5:11 PM
02/03/09

Rock Castle Construction
Voided/Deleted Transactions Detail
All Transactions

Num	Action	Entered/Last Modified	Date	Name	Memo	Account	Split	Debit	Credit
Transactions entered or modified by Admin									
Check 304									
▶ 304	Deleted Transaction	02/03/2009 17:11:37						0.00	◀
304	Changed Transact...	02/03/2009 16:21:26	11/17/2008	A Cheung Limited A Cheung Limited		Checking Job Expenses:Job...	Job Expense... Checking	5,000.00	5,000.00
304	Added Transaction	11/17/2008 09:36:22	11/17/2008	A Cheung Limited A Cheung Limited		Checking Job Expenses:Job...	Job Expense... Checking	500.00	500.00
Deposit									
	Voided Transaction	02/03/2009 17:11:48	11/17/2008	A test	VOID: Depo...	Checking Construction Incom...	Construction ... Checking	0.00 0.00	
	Changed Transact...	02/03/2009 16:21:33	11/17/2008	A test	Deposit	Checking Construction Incom...	Construction ... Checking	350.00	350.00
	Added Transaction	11/17/2008 09:35:30	11/17/2008	A test	Deposit	Checking Construction Incom...	Construction ... Checking	550.00	550.00

Previous Reconciliation Reports

Another key way to detect fraud is to keep accurate banking and credit card reconciliation reports and carefully review the reconciliations. QuickBooks Premier and Enterprise Solutions allow you to prepare Previous Reconciliation reports for any prior period. However, QuickBooks Pro only provides the most recent previous reconciliation report. These static Previous Reconciliation reports (stored as Adobe PDF files) show the exact detail of your cleared and uncleared transactions that were marked when performing reconciliations. This report can be coupled with the Reconciliation Discrepancy report that allows you to track all of the changes users make to reconciled transactions.

7:45 PM
12/15/07

Rock Castle Construction
Previous Reconciliation Discrepancy Report

Checking

Type	Date	Entered/Last Modified	Num	Name	Reconciled Amount	Type of Change	Effect of Change
Statement Date: 11/14/2007							
▶ Check	11/12/2007	12/15/2007 19:45:37	236	Patton Hardware S...	-48.10	Amount	-432.00
Transfer	11/14/2007	12/15/2007 19:45:12			2,500.00	Amount	-2,250.00
Total 11/14/2007							<u>-2,682.00</u>
							<u><u>-2,682.00</u></u>

This is important for internal controls, because the person doing the bank (or credit card) reconciliation should be different from the users/employees who enter cash disbursements (e.g., checks, bill payments, sales tax payments, paychecks, and payroll liability payments) and banking deposits—especially for deposits that contain customer payments.

If there are fraudulent activities around the disbursement of cash, the user performing the bank (or credit card) reconciliation will be in a position to detect this fraud. If users attempt to modify transactions that a user reconciled—after the reconciliation is completed—their changes will post to a very specific report. Also the beginning bank balance on the bank reconciliation window will no longer tie to the bank.

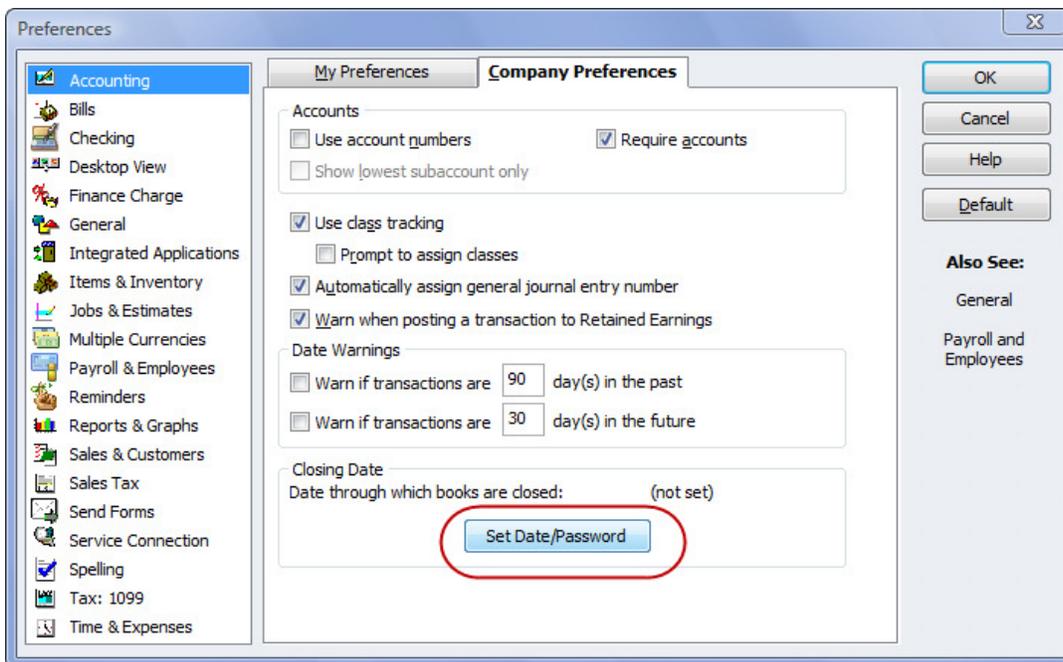
The person doing the reconciliations can refer to the static reports to show that the accounts did indeed tie to the bank at the time of the reconciliation. The company can use a combination of the static bank reconciliation reports, the Previous Reconciliation Discrepancy report, the Voided/Deleted Transaction report, and the Audit Trail report to locate the exact actions of the fraudulent users and which user performed the action.

Controlling Transactions in Closed Periods

Preventing new transactions from being posted in closed periods and preventing existing transactions in closed periods from being changed or deleted has long been a major concern of many QuickBooks users. However, implementing effective internal control in this area can be relatively easy and effective. A four-step approach will be utilized to prevent transactions in closed periods from being added, edited, or deleted without appropriate authorization:

1. Set the Closing Date
2. Establish a Closing Date Password
3. Restrict access to prior periods when user profiles are created
4. Utilize the Closing Date Exception Report

The Closing Date is the date through which the books are deemed to be closed; it can be any date, but is usually set to be the last day of a month, quarter, or year. With the Closing Date set, whenever a user tries to enter, edit, or delete a transaction in a closed period, the user is warned that the transaction will impact a closed period and is prompted to confirm that this is the desired outcome. To set the Closing Date, access the Accounting Preferences window and enter the Closing Date, as shown below. Note that only the Administrator user or a user with Sensitive Accounting Activities rights can change the Closing Date.



In addition to setting the Closing Date, the Closing Date Password should be established. Once the Closing Date Password is established, only those who know this password are allowed to enter, edit, or delete transaction in periods deemed to be closed by the Closing Date.

With the Closing Date Password established, whenever a user attempts to enter, edit, or delete a transaction in a closed period, the user is prompted to enter the Closing Date Password. If the user enters the correct password, the transaction impacting the closed period can be completed; if the user does not enter the correct password, the transaction cannot be completed.

For obvious reasons, only a very small number of persons should know what the Closing Date Password is for a given company. And, should the Closing Date Password ever become compromised, it should be changed immediately.



An additional measure of internal control preventing transactions in closed periods from being changed or deleted centers on the rights granted to each QuickBooks user. When establishing user rights, by not granting a user the right to change or delete transactions in closed periods, as shown in the image below, the user will not be able to change or delete any transaction in a closed period even if the user knows the Closing Date Password. If this is applied to all user profiles, then the only user who will be able to change or delete transactions in closed periods is the Administrator. Note, however, that this right does not extend to entering new transactions in closed periods; that is, as long as a user knows the Closing Date Password, then new transactions can be entered in closed periods. This is why it is important that only users that should be properly making adjustments to closed periods should know the closing date password.



One very effective internal control measure to assist in detecting which transactions may have been entered, edited, or deleted in closed periods is the **Closing Date Exception Report**. Similar in design to the Audit Trail Report, the Closing Date Exception Report provides a summary of all transactions dated on or before the Closing Date that were added, changed, or deleted after the Closing Date was established. Accessed by selecting **Reports, Accountant & Taxes, and Closing Date Exception Report** from the menu, this report also provides a record of every time the **Closing Date** was changed, as shown in below.

Modify Report... Memorize... Print... E-mail Export... Hide Header Refresh

4:16 PM
02/03/09

Rock Castle Construction
Closing Date Exception Report
Books are currently open

Num Entered/Last Modified Last modified by State Date Name Memo Account Split Debit Credit

Closing Date History

Closing date cleared on 12/15/2007 20:54:54 by Admin
 Closing date set to 09/30/2007 on 12/15/2003 18:00:00 by Admin
 Closing date set to 09/30/2003 on 12/15/2003 15:07:00 by Admin

Transactions entered or modified by Admin

Num	Entered/Last Modified	Last modified by	State	Date	Name	Memo	Account	Split	Debit	Credit
Bill										
	12/15/2007 17:15:42	Admin	Latest	03/15/2007	East Bayshore Au...	VOID: Mon...	Accounts Payable	Automobile:R...	0.00	
					East Bayshore Au...	Transmissi...	Automobile:Repair...	Accounts Pa...	0.00	
	09/25/2002 13:54:25	Unknown user	Prior	03/15/2007	East Bayshore Au...	Monthly Truc...	Accounts Payable	Automobile:R...		942.90
					East Bayshore Au...	Transmission...	Automobile:Repair...	Accounts Pa...	942.90	
Bill										
	12/15/2007 15:58:27	Admin	Latest	05/01/2007	Kershaw Compute...		Accounts Payable	Computers		13,000.00
					Kershaw Compute...	Desktop PC ...	Computers	Accounts Pa...	13,000.00	

Using Reports to Detect Billing Scheme Frauds

Among the more common forms of fraud committed against small businesses involves billing schemes². Examples of these schemes include:

- Perpetrators cause fictitious invoices from non-existent vendors to be paid; the perpetrator (or their friend or relative) actually receives the payment.
- Paying invoices on multiple occasions or in inflated amounts; the perpetrators then receive and cash the refund checks.
- Paying for purchases from vendors that were for products used personally.

In some cases, utilizing a purchase order system will prevent these types of fraud from being committed; however, in many small businesses this is unlikely as purchase order controls typically depend on segregation of incompatible duties to be successful. Unfortunately this will not be the case for many small businesses, including many of those running QuickBooks. Therefore, attention should be directed to detective control measures, including careful and critical reviews of key reports.

Examples of QuickBooks reports that can be useful in detecting billing scheme frauds include:

- Transaction List by Vendor
- Check Detail
- Audit Trail
- Purchases by Vendor Detail
- Purchases by Vendor Summary
- Purchases by Item Summary
- Purchases by Item Detail
- Open Purchase Orders
- Budget vs. Actual

In addition, more experienced users may want to examine using third-party software to write even more specific reports that Open Database Connectivity (ODBC) connections to query the QuickBooks database for details not available in standard QuickBooks reports. For example, a report could be written in Excel to report all payments made to vendors where the vendor has been added to the Vendor List within the past ninety days.³

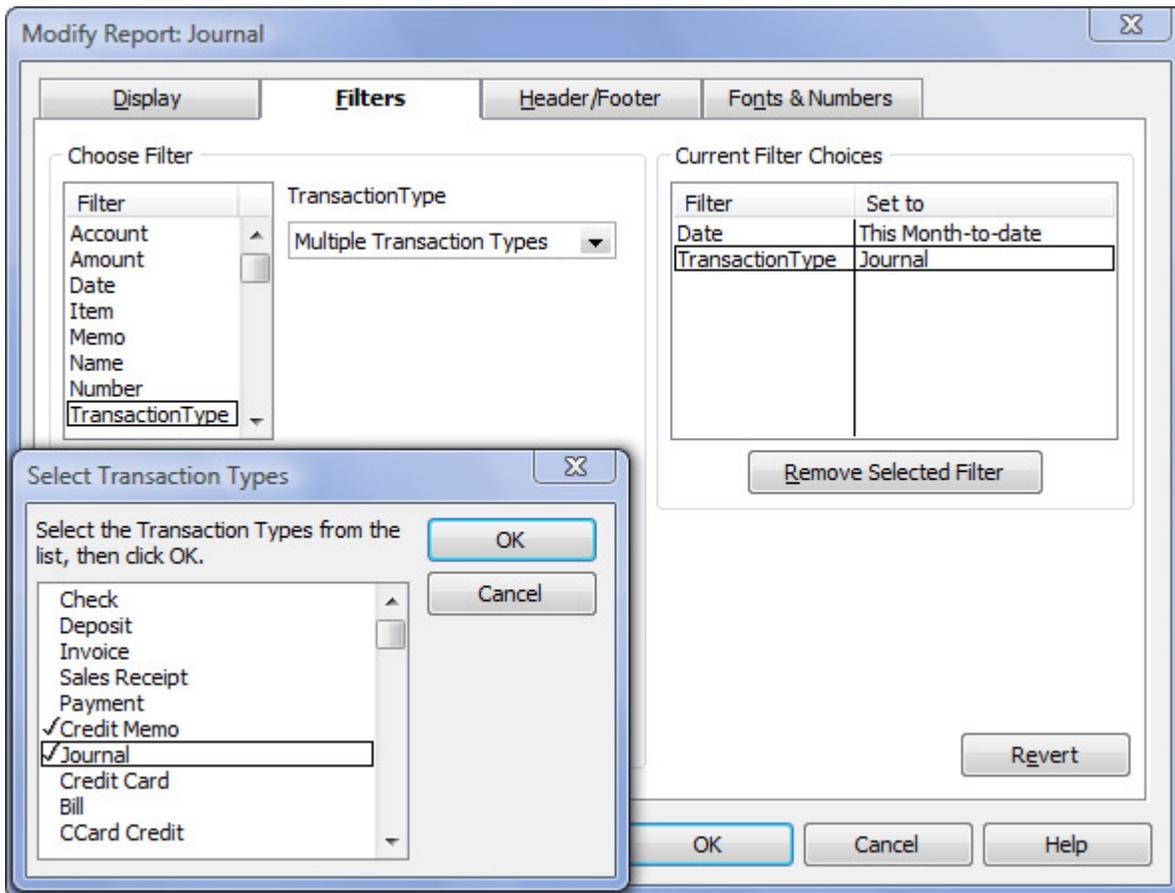
² According to the 2004 Report to the Nation on Occupational Fraud and Abuse, billing schemes account for 33% of all reported occupational frauds for small businesses. Additionally, the median loss to businesses for billing scheme frauds was \$140,000.

³ Such a report would be dependent upon establishing an ODBC connection between QuickBooks and Excel. To do so, an ODBC driver such as QODBC would be required. For more information, visit www.qodbc.com or www.flexquarters.com

Using Reports to Monitor Bad Debt Write-offs

As with billing schemes, it will often be necessary to utilize QuickBooks reports to monitor bad debt write-offs and other adjustments to customer accounts. Without careful monitoring of these types of transactions and in the absence of segregation of duties, it might be possible for an employee to receive a customer payment, keep it for personal use, and write-off the customer payment as a bad debt, or simply delete the customer invoice if the employee's permissions allow them to do so.

Perhaps one of the best reports to do this, in addition to the Audit Trail Report, would be a Journal. In its standard format, a Journal is a listing of all transactions occurring during a given time frame. To view a Journal, select **Reports, Accountant & Taxes, and Journal** from the menu. Next, filter the report to show only Credit Memo and Journal transactions by selecting Modify Report and clicking the Filters tab. Under the Filters tab, set Transaction Type to Selected Transaction Types and then select Credit Memo and Journal from the drop-down list as shown below.



Budgetary Controls

Budgets should play a major role in internal control procedures in virtually every company, including those utilizing QuickBooks. Effective budgetary control can provide early warnings to business owners and managers when key business objectives are in danger of not being met. To that extent, QuickBooks supports entry of budget data and reporting of actual results compared to budget numbers. Entry of budget data is initiated by selecting **Company, Planning & Budgeting, Set Up Budgets** from the menu. Monthly budget data is entered on an account-by-account basis in the spreadsheet grid depicted in the image below. Notably, this data can be entered for balance sheet accounts as well as income statement accounts and can be further segmented by customer or class if so desired.

Account	Annual ...	Jan10	Feb10	Mar10	Apr10	May10	Jun10	Jul10	Aug10	Sep10	Oct10	Nov10	Dec10
Mileage Income													
Construction Income													
Discounts given													
Labor													
Materials													
Miscellaneous													
Subcontractors													
Uncategorized Income													
Freight & Delivery													
Cost of Goods Sold													
Automobile													
Insurance													
Fuel													
Repairs and Maint...													
Bank Service Charge													
Bank Service Charges													

Budget reports are accessed from the **Reports** menu by selecting the **Budgets & Forecasts** option. One of the more effective reports is the **Profit & Loss Budget vs. Actual** report which depicts monthly and annual budgeted data, actual results, and both dollar and percentage deviations. Business owners and managers should monitor this report very closely for negative or unexpected trends.

Customer Credit Card Protection

QuickBooks allows you to protect not only your business finances, but other important information such as your customer's credit card numbers. The software gives you several layers of customer credit card protection, which include using complex passwords to access credit card numbers. It also includes a new report, the Credit Card Audit Trail report that tracks usage, including the viewing, of customer credit card numbers.

If you process credit cards using QuickBooks Merchant Services or if you store credit card information in the Payment tab of the Customer Setup window in QuickBooks, you need to comply with security standards governed by the PCI DSS (Payment Card Industry Data Security Standard). Failure to do so could result in severe fines if the credit card information should fall into the wrong hands.

The QuickBooks Customer Credit Card Protection feature requires the QuickBooks administrator user to enter a complex QuickBooks password that is at least seven characters and includes at least one uppercase letter. To comply with PCI DSS, QuickBooks will prompt you to change the password every 90 days.

When you select the Company drop-down menu and then select Customer Credit Card Protection, QuickBooks asks if you want to enable Customer Credit Card Protection and then displays the window shown below. When you setup the more complex password, you also enter a challenge question and answer.

Customer Credit Card Protection Setup

Create Complex QuickBooks Password

To complete customer credit card protection setup, create a new complex QuickBooks password that you must change every 90 days. [Explain](#)

All Fields required

User Name: Admin

New Password: •••••••• Requires at least 7 characters, including one number and one uppercase letter

Confirm New Password: ••••••••

Example: coMp1ex

Set Up Password Reset

Select a challenge question and enter answer. [How will this help me reset my password?](#)

Challenge Question: Name of your high school

Answer: _____

Answer is not case sensitive

OK Cancel

Note: You can set up complex passwords for additional users with access to credit card information. However, you cannot use the QuickBooks Customer Credit Card Protection Feature to regulate the passwords for these users. Instead, the administrator can either reset each user's password or can set an office policy requiring users to change their passwords every 90 days—to comply with PCI DSS.

The Customer Credit Card Audit Trail tracks each time a QuickBooks user enters, displays, edits, or deletes credit card information. The report also tracks each time a QuickBooks user makes changes to the QuickBooks Merchant Services subscription. Only the administrator can view the Customer Credit Card Audit Trail, and QuickBooks does not allow you to filter or memorize the report. Also, the Customer Credit Card Audit Trail is available only if you enable the customer Credit Card Protection feature.

Understanding Key Preferences

Many QuickBooks preferences have internal control implications; accordingly due care and consideration should be given whenever establishing or changing preferences for a QuickBooks data file. In this section, some of the more relevant preferences regarding internal control are reviewed.

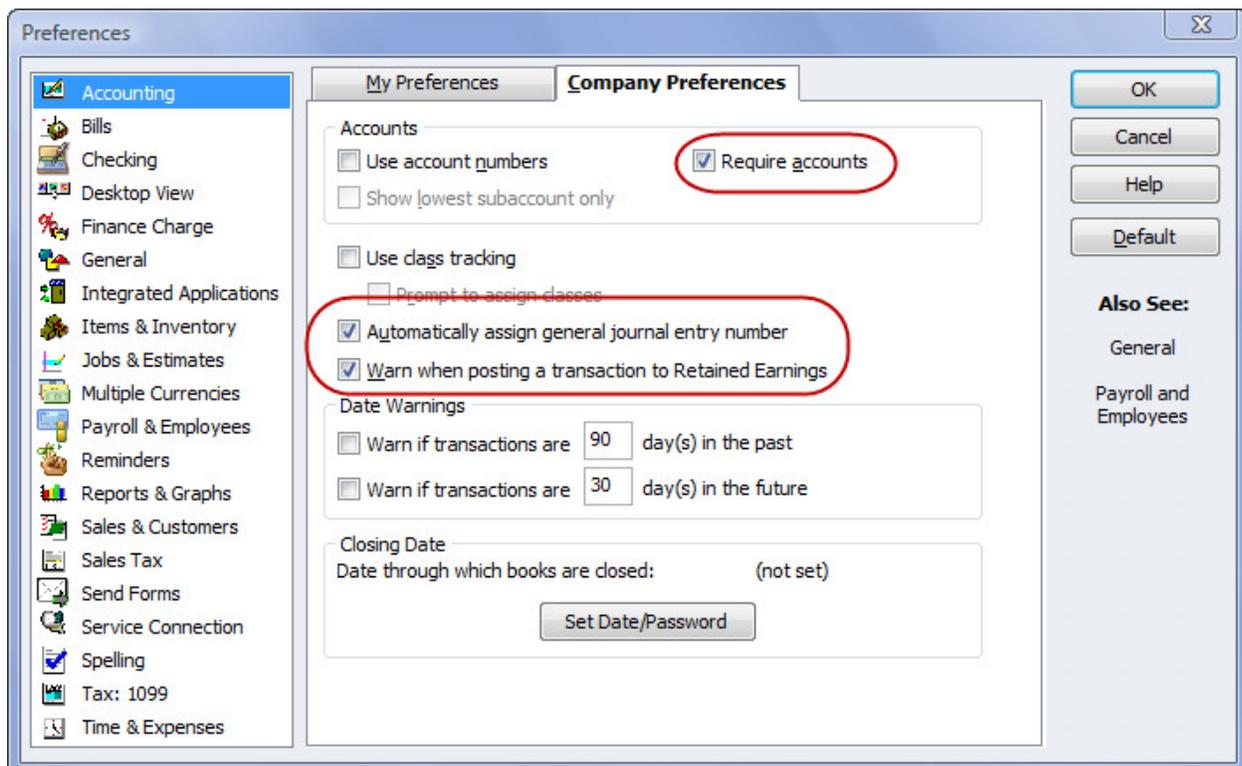
Accounting Preferences

As a guideline, most QuickBooks companies should activate all of the Accounting Preferences, with the possible exception of **Use class tracking**.

Some of the more significant Accounting Preferences are **Require Accounts**, **Automatically assign general journal entry number** and **Warn when posting a transaction to Retained Earnings**.

Note – we can't think of any legitimate daily transaction that should be posted to Retained Earnings, so letting the bookkeeper know to stay away from this account is probably a good thing.

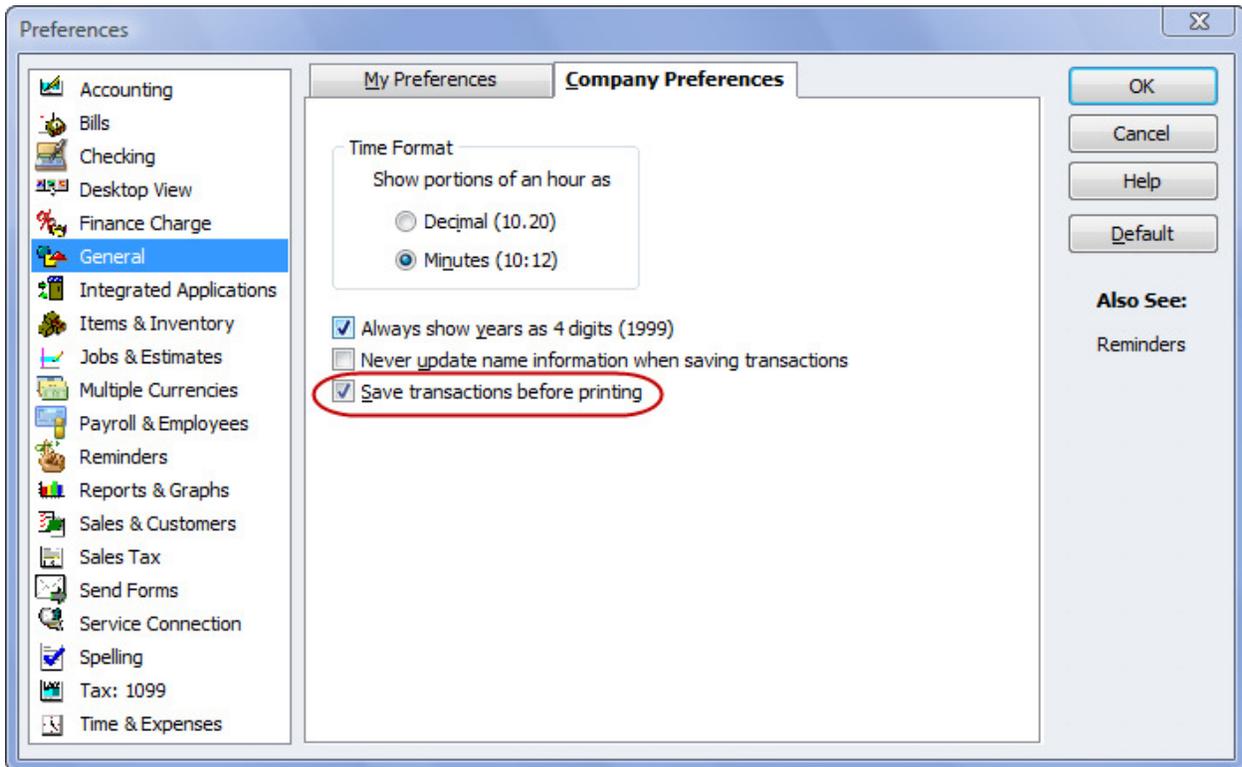
Activating **Require Accounts** prevents users from accidentally posting transactions to either Uncategorized Income or Uncategorized Expense. **Automatically assign general journal entry number** is a good practice. **Warn when posting a transaction to Retained Earnings** provides a warning message to users when attempting to post a transaction to Retained Earnings, though the transaction may still be posted, if desired. (Again, educating the bookkeeper is the best line of defense here.)



General Preference

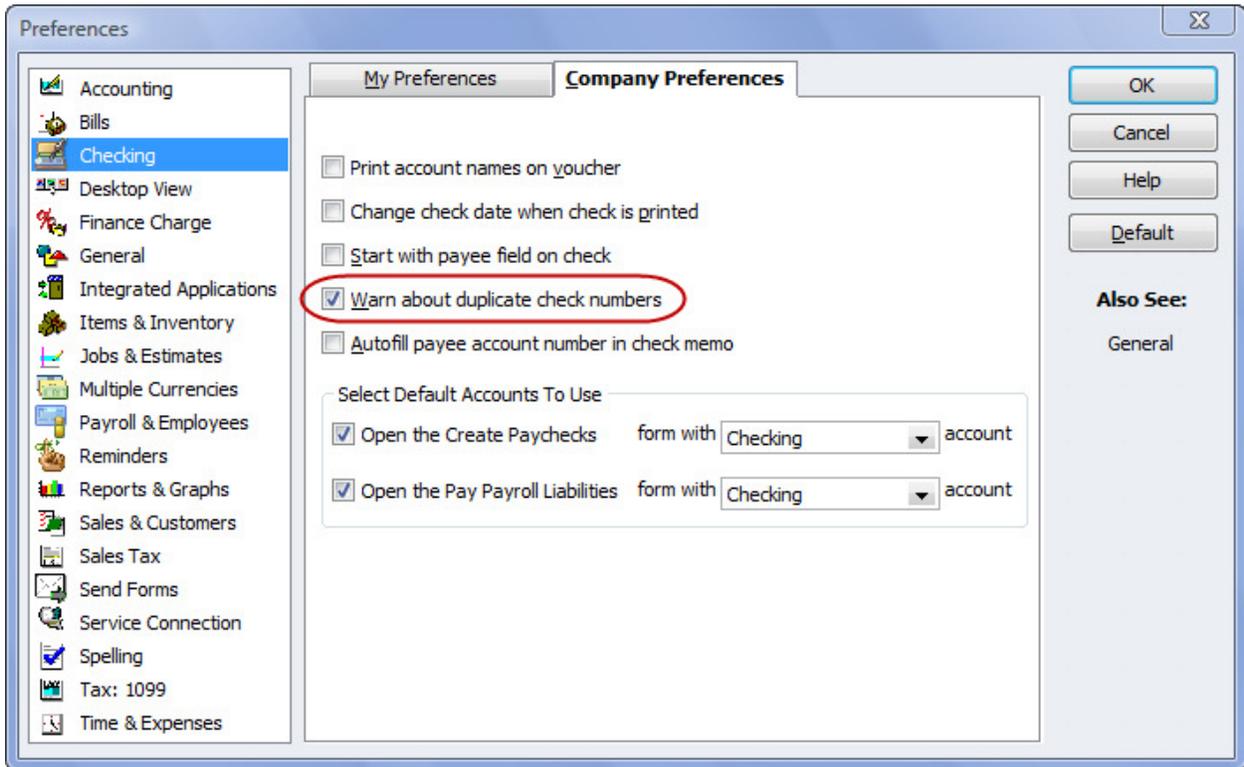
Many company-level Preference settings in QuickBooks help to protect your business from fraud. One preference to pay particular attention to is **Save all transactions when printing**. By ensuring that all transactions are saved when printing, you can avoid specific types of fraud. Here's an example of how fraud could occur if a user/employee could print a transaction without saving it:

An employee could create and print an invoice to a customer, and then send it (or hand it) to the customer, but never hit "save" in QuickBooks. So when the customer pays the business for the services or goods, there is no record of the transaction anywhere in the financial management software. The employee can then pocket the money, and the transaction goes undetected. The upside is that QuickBooks always saves paychecks as they are printed. But for other transactions, such as invoicing, the Save When Printing feature has to be specified as a Company Preference in the software.



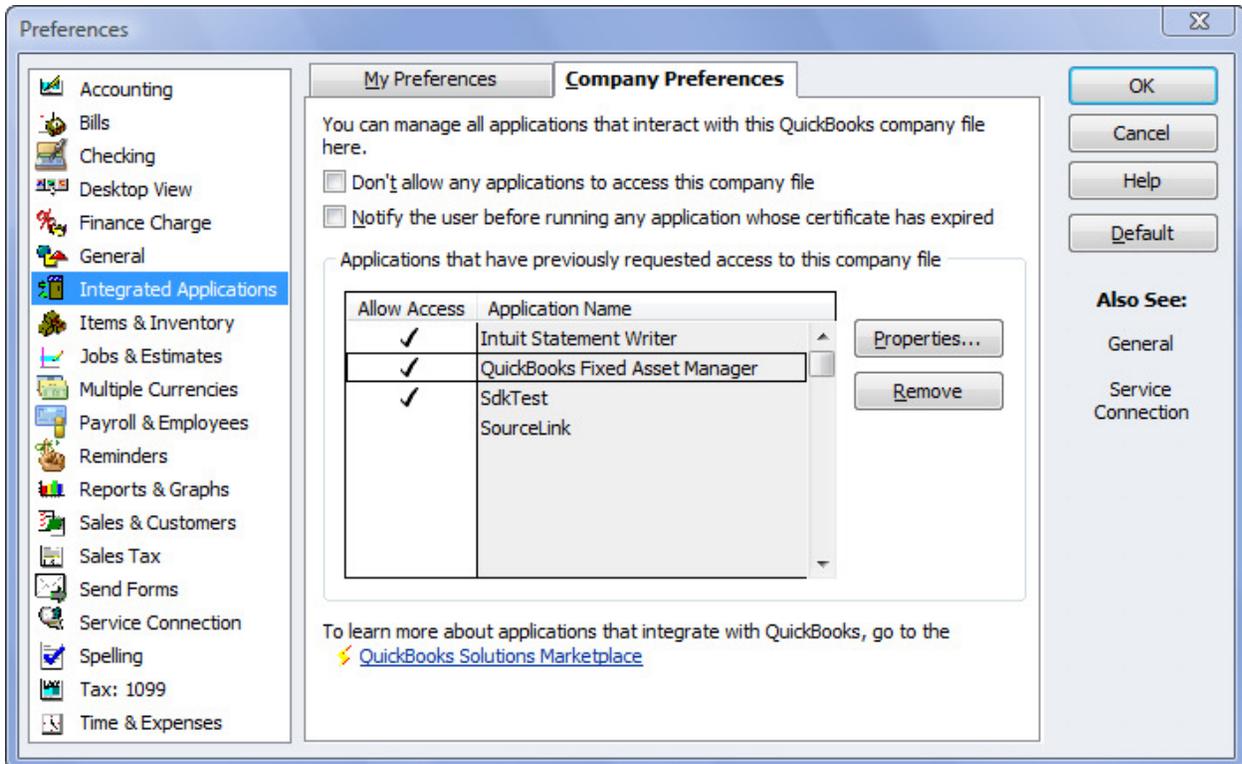
Checking Preferences

Among the key Checking Preferences is **Warn about duplicate check numbers**. Generally, this preference should be activated to provide a warning that a check number is about to be used on multiple occasions. The warning generated is a “soft” warning; that is, the duplicate check number can still be used. Also, other key preferences related to internal control include the ability to specify default accounts for paychecks and payroll liabilities.



Integrated Applications Preferences

QuickBooks provides the ability for third-party software applications to access and interact with QuickBooks data files. Examples of such applications would include those which generate magnetic media filing of Forms W-2 and 1099. However, most companies do not utilize such applications; therefore, the recommended setting for these companies is to check the box labeled **Don't allow any applications to access this company file** or you may allow access to Intuit Statement Writer, Fixed Asset Manager or others as needed. Failing to control access to the QuickBooks data file through this setting can lead to unauthorized access to the data file and occupational fraud.

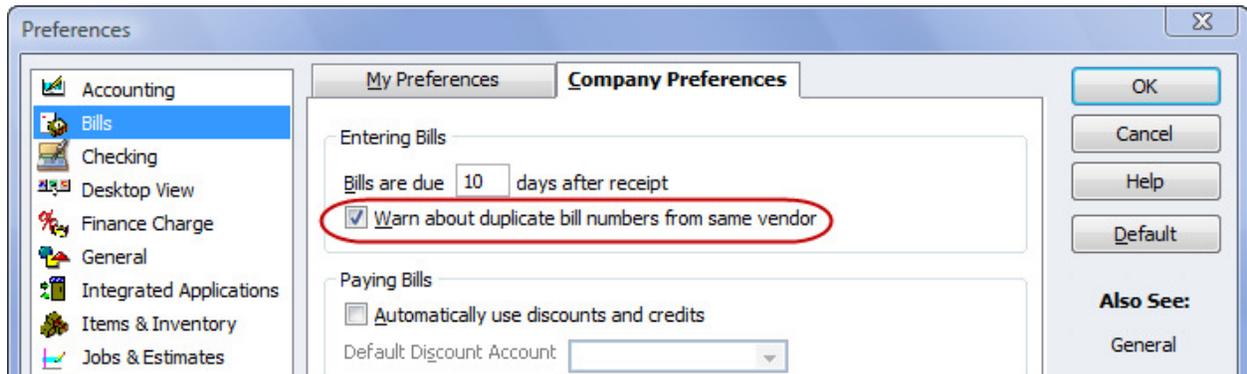
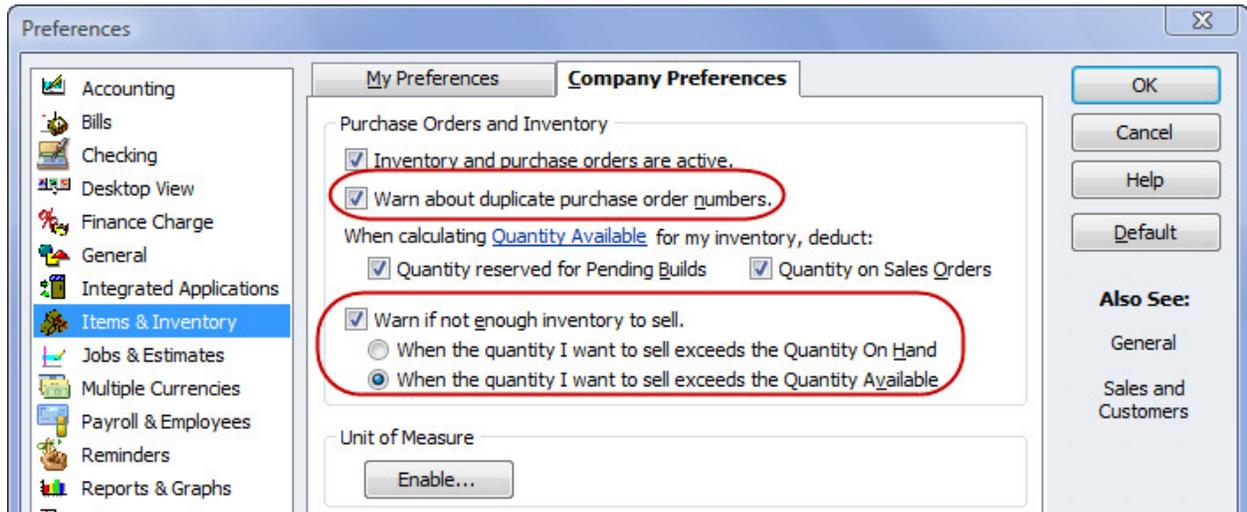


Items & Inventory and Bills Preferences

There are a number of significant preferences related to Items & Inventory and Bills. Key preferences in this category include:

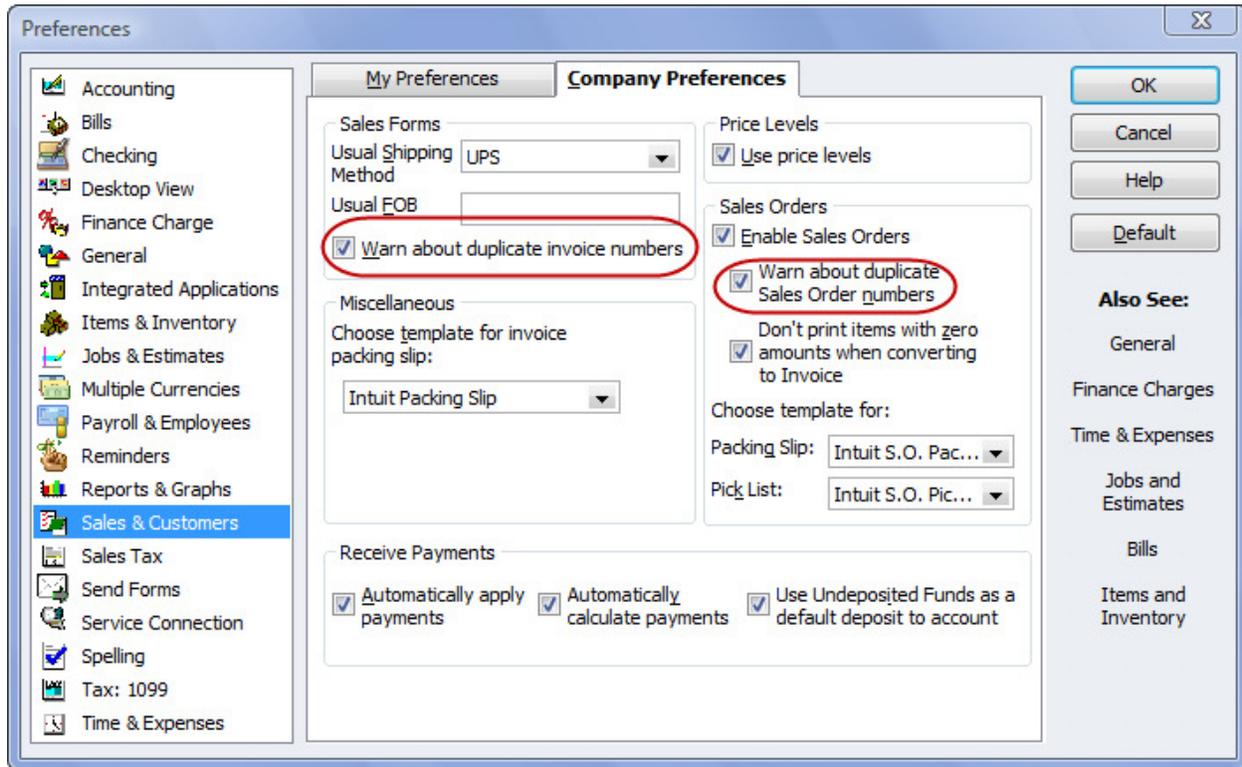
- Warn about duplicate purchase order numbers.
- Warn if not enough inventory quantity on hand (QOH) to sell.
- Warn if item quantity exceeds QOH less quantity on Sales Orders.
- Warn about duplicate bill numbers from same vendor.

For maximum internal control, each of these preferences should be activated, as shown below.



Sales & Customers

As with Purchases & Vendors Preferences, a number of key Sales & Customers Preferences impact internal control. The two most significant among these are **Warn about duplicate invoice numbers** and **Warn about duplicate Sales Order numbers**. For maximum control, both of these preferences should be activated as shown below, thereby reducing the possibility that a form number is used on multiple occasions.



There are other preferences that impact internal control in a QuickBooks installation and the preceding discussion is not intended to be a complete review of all preferences or even those that impact internal control. Rather, this is intended to provide some insight into those preferences that have the greatest impact on internal control in a QuickBooks setting and provide recommended settings for these preferences. The QuickBooks Administrators and other users are strongly encouraged to understand the impact of all QuickBooks preferences, including those labeled **My Preferences** and make adjustments as appropriate based on individual circumstances.

QuickBooks: Online Banking and Bill Pay

Online account access lets your clients manage their cash (and credit cards) in the same place where they keep track of it—in QuickBooks. They won't have to leave their desk or even pick up the phone to perform the following various functions—such as:

- See which checks have cleared
- View the current balances for all online bank accounts
- Transfer funds between accounts at the same financial institution
- Apply for online banking services online
- Transmit Bill Payments to your financial institution for payment
- Download credit card transactions

Financial institutions provide different levels of online banking service. Some do not offer it at all. Others provide enhanced services, such as allowing QuickBooks to transfer money between two online accounts. Check with your financial institution to see what services it offers. Some offer Web connect that allows you to download transactions into a file and import them into QuickBooks. Others offer Direct connect (for a fee) which allows automatic downloading of transactions into QuickBooks and you can initiate transactions (ie payments to send) from within QuickBooks too.

The use of online banking will allow the small business owner to stay more involved with the day to day cash transactions and the vendor bill payments. It will also allow business owners more flexibility to where they can work on their business. And, they can have complete control over what payments get made to what vendors. But it is important that the owner maintains an active role and does not allow the bookkeeper (or anyone) full access without proper controls and oversight.

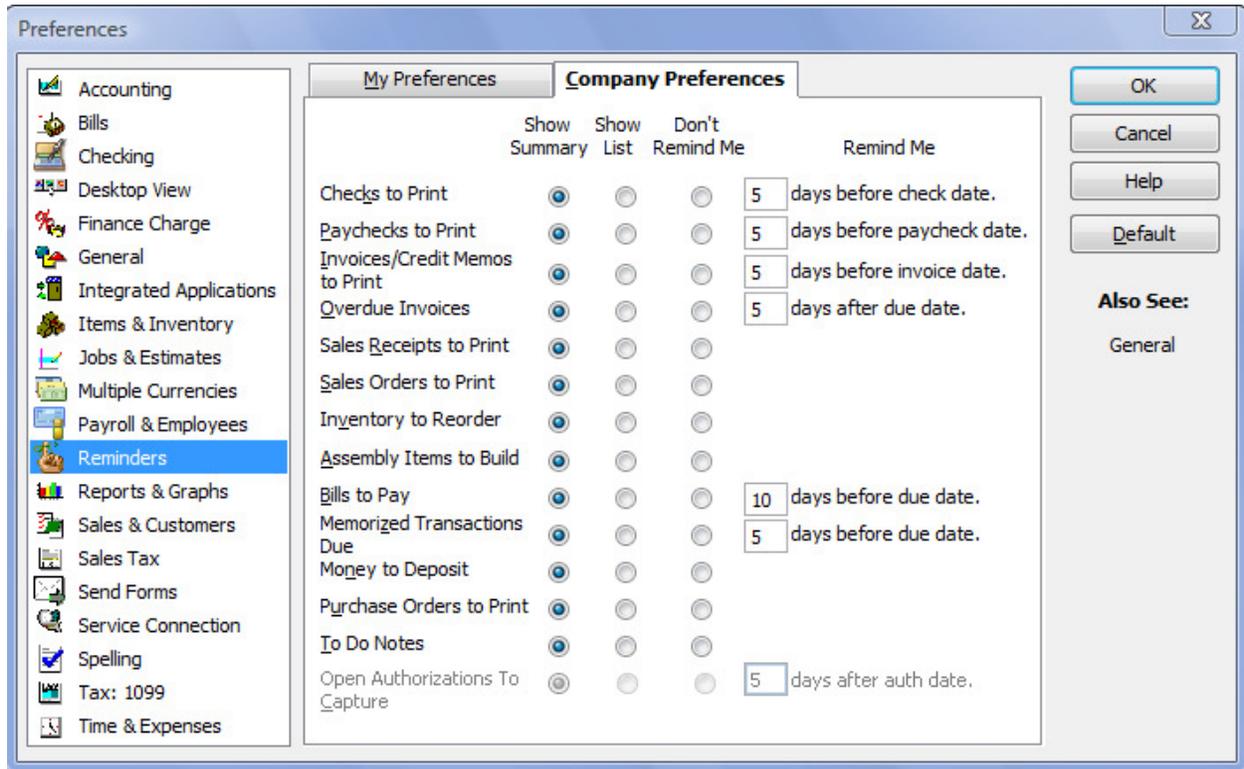
The screenshot displays the QuickBooks Online Banking interface. At the top, there are links for 'Contact Info', 'Video Tutorial', and 'Renaming Rules'. The main section is titled 'Financial Institution' and shows a dropdown menu set to 'ANYTIME Financial'. Below this, there are two columns: 'Online Accounts' and 'Online Balance'. The 'Online Accounts' column lists 'Checking' with a balance of '\$5,035.66' and 'Savings' with a balance of '\$0.00'. A 'Send/Receive Transactions' button is prominently displayed in the center. Below this, there are two sections: 'Items Ready To Send(2)' and 'Items Received(7)'. The 'Items Ready To Send' section includes a list of actions like 'Write Online Checks', 'Pay Bills', 'Transfer Funds', etc., and a table showing transaction types and their totals. The 'Items Received' section includes a table showing items to review, such as 'Checking' with 7 items to review and a balance of \$43,741.98.

Transaction Type	No. To Send	Total
Online Checks (0)	0	\$0.00
Bill Payments (1)	1	\$625.00
Transfers (1)	1	\$500.00
Messages (0)	0	
Payment Inquiries (0)	0	
Payment Cancellations (0)	0	

Item	No. To Review	QuickBooks Balance	Online Balance
Checking	7	\$43,741.98	\$5,035.66
Savings	0	\$0.00	\$0.00
Messages Received	0		
Payment Inquiry Re...	0		
Alerts	0		

Monitoring Due Dates with Reminders

Missed due dates for tax return filings, tax deposits, even customer, vendor, or employee meetings can be minimized by effectively using the Reminder List. Configuring the Reminders Preference allows users to specify when Reminders are displayed and how much detail is provided when the Reminder is displayed.



In addition to QuickBooks-generated Reminders, user-defined Reminders can be created through the To Do Notes function. For instance, a To Do Note could be created for a customer, job, vendor, or employee reminding a business owner of a key task or event. The To Do Note will appear in the Reminder List, based on the Reminders Preferences as shown above.

Verify Data Integrity

QuickBooks software offers an important tool that will allow your clients to ensure that their data integrity remains intact. To run this important tool, click on **FILE...UTILITIES** and then click on **Verify Data Integrity**. If data has lost integrity the **Rebuild Data** tool can then be run through the same menu. Another feature in QuickBooks is that when you are backing up QuickBooks you can select an option to verify data integrity whenever the backup is made. This may slow down the backup process slightly but will help to ensure overall system integrity

QuickBooks Auto-update

After Intuit releases a new version of its software, their quality engineers stay dedicated to making sure the product has all of the features and controls it needs. Periodically throughout the year they may release a free downloadable update to the software. This update may change the performance of the software or fix a small bug. In either case it is important to make sure that your clients download and install these updates. QuickBooks has made this easy through the **Auto-update** feature. To make sure this feature is turned on. First go to the **Help** menu and click **Update QuickBooks**. The Update QuickBooks window will appear. Next click the **Options** tab, finally make sure that **Yes** is selected for the **Automatic Update Option**. For this option to work, you do need to be connected to the internet.

Effective Backup Procedures

Businesses of all sizes should implement effective backup procedures to safeguard against catastrophic loss of data.⁴ Small businesses, including those running QuickBooks, are no exception to this rule. Unfortunately, empirical evidence suggests that many small businesses don't backup their data at all.⁵

Backups should always be stored offsite. Too many times clients keep their only backup in the drawer next to the computer; or even worse they only backup to the hard drive. In the case of fire or other disaster; the backup would be destroyed along with the original data. The backup should be taken home or stored in a safe deposit box instead.

QuickBooks users should strongly consider using an off-site backup option. QuickBooks offers an online backup service as an add-on service which ensures the data is backed up on a regular basis to an off-site location. This will help eliminate the issues of the backup not working, not being made at all, or being destroyed in the event of a disaster.

For those QuickBooks users who will continue to backup data locally, a few key points are worth reviewing.

- A backup schedule acceptable to the individual business should be established and followed. (Think about how much data it would be acceptable to have to re-enter, and plan the schedule around that number of transactions – typically daily or weekly.)
- Backup media should be stored off-site
- At least three different generations of backup media should be utilized
- Backup media should be replaced periodically
- Backups should be tested periodically to verify that files can be restored in the event of a loss of data
- Duplicate back up methods may be advisable

Regardless of whether data will be backed up over the Internet via an on-line backup service or backed up locally to CD, or other media, small business owners and managers should pay very careful attention to this issue and ensure that key business data – including QuickBooks data – will be available when it is required.

In QuickBooks, the data file should also periodically be verified and rebuilt to ensure the integrity of the database to prevent data corruption issues encountered in large databases. It should be done on a periodic consistent basis. A good recommendation is to run this verification and rebuild each month after the bank reconciliation is complete. Running data verification often will allow the software to alert you of any problems with the database and give you the opportunity to fix them while they are still small.

⁴ According to U.S. DataTrust, 90% of all businesses that lose their data are out of business within two years.

⁵ The number of small businesses that do not backup their data at all was estimated at forty percent in a study by Gartner.



Choose the file type based on how you will use the file.

Use a backup copy to protect against accidental loss of data.

A backup contains everything you need to re-create your company file and QuickBooks environment, including all of the QuickBooks files (templates, letters, logos, images, and so on) related to your company file. In case of accidental loss or damage, you can use the backup file to restore your company data. Unlike a portable file, a backup file is very large and cannot be e-mailed. It is not recommended as a means of moving company data, unless you have a new computer and need to move all of your related files as well.

Use a portable company file to e-mail or temporarily move your data.

A portable company file is a compact version of your company file, small enough to send by e-mail or save to portable media. A portable file contains only your company file financial data. Unlike a backup file, it doesn't contain related files such as letters, logos, images, and templates. It also doesn't contain a transaction log (.tlg file) which can be used to restore transaction data with the help of Intuit Technical Support, if damage or loss occurs.

Use an Accountant's Copy to exchange files with your accountant.

With Accountant's Copy you can work on your company file at the same time as your accountant. You continue to work with your company file, while your accountant makes adjustments to a special version of the company file called an Accountant's Copy. Changes made by the accountant can later be imported into your current company file.