Individualized Systems, LLC
Your De-Tax Professionals

Tax Tips

Internal Controls for the Small Business

Introduction:

You've heard it: "98% of all businesses go out of business in their first year." You may even have heard the why: "... as a direct result of bad records". What you don't hear is that for a vast majority of these businesses, the bad records are the result of or result in fraud, theft and embezzlement of precious resources, like cash, that the business needs to stay in business. Unfortunately, "White Collar" crimes, including fraud and embezzlement, increase every year and mostly hit small businesses whose numbers are increasing at a dramatic rate.

So, what exactly are "Internal Controls"? They are steps taken by a company to ensure that the assets of the company (specifically inventory and cash) are kept safe for the use of the company and don't walk out the door in an employee's or customer's pocket.

Because of their smaller size, their financial contstraints in having an in-house accountant and because they are not required to have yearly audits which might catch many control problems before they become dangerous, small and closely-held businesses have a significantly greater risk for loss even though their ability to sustain the loss is smaller. El Paso statistics indicate that over 50% of reported cases involve check forgeries. One small business lost $150,000.00 to forged checks before the problem was discovered. To date, the employee in question is still at large. Another lost nearly 50,000 to credit card fraud and, again, the perpetrators have not been apprehended. This type of loss can seriously cripple or even close a small business.

Information on internal controls has been primarily aimed at Auditors and/or the Corporate Structure. Unfortunately, the controls available to these larger companies are not possible for the small business because of the lack of personnel. Therefore, it is all the more important for individually-owned businesses to have guidelines which the owner/manager can rely upon to check the internal controls, especially if the business records are kept on a computer system.

The below discussion is intended not only to impart information, but also as a tool by small businesses for use in evaluation the internal controls of a small business on an automated system. We strongly recommend you print this out and provide a copy to your accountant who can then evaluate your small business controls and make recommendations for improvements.

Although many small businesses cannot afford and, in reality, do not need all of the controls mentioned in this discussion, most need a thorough review of their controls and, at the very least, a few, minor changes in existing standards which will improve the handling and protection of their most valuable resources - their assets.

Part I: Small Business & Internal Controls
Definitions & Characteristics

Definition of Small Business

There is no exact definition of a "Small Business". The SBA (Small Business Administration) defines it as a company which earns less than $1,000,000.00 per year. However, it seems the term in practice does not relate to the actual size of the business as much as to specific characteristics of it's management and operations:

1. Management personnel consist primarily of one or two key executives whose talents lie in marketing (advertising), manufacturing (building), or non-financial services (insurance, food services).

2. The business is owned by management and/or its families with all the affairs of the company dominated by the executives.

3. Management attitudes towards accounting and record-keeping (it is needed for taxes and, sometimes, the bank) are not geared to hiring employees with expertise and education in this area.

4. Internal controls are limited or nonexistent and the controls that may exist are readily overridden by management.

5. The business tends to be uncomplicated with easily-identifiable systems and consistent operations.

6. Policies, procedures, and responsibilities are communicated by word of mouth and, rarely written.

Internal control consists of three primary elements:

1. Environment
   The environment is the effect of factors outside the system such as: the number of employees, the actual type of business, the culture surrounding the business and the community it is in.
2. Procedures
   Procedures are the policies and programs which are established to povide assurance that management goals are achieved (who does what, how and when)
3. Accounting system
   The accounting system consists of the processes and records that identify, assemble, analyze, classify, record and report the transactions of the business and maintain responsibility for the assets and liabilities.

Establishing controls for a business must necessarily consider the size; characteristics and nature of the business; the complexity of its operations; current and desired processing methods; and any applicable legal and regulatory requirements**.**

The characteristics of an effective and productive system of internal controls:

This information comes directly from internal control and auditing manuals which are, unfortunately geared towards larger companies. However, in order to create a good system for a small business, one must first understand how a 'perfect' system works so that the smaller business can strive for the maximum similarity it can achieve within its individual financial and size constraints.

1. Appropriate segregation of responsibilities:
   A) Custodial:
      Person(s) with direct access to physical assets.
   B) Recordkeeping:
      The Person(s) who record and keep the transaction records
   C) Authorization:
      Person(s) with authority to approve transactions.

   If any two of these duties are combined, the assets are at risk.

2. Clearly defined lines of authority:
   The business should be structured to insure each person is held accountable for specific assets, liabilities or activities with clearly defined authority lines.

3. Adequately qualified personnel:
   Consideration must be given to the qualifications needed to perform the duties of each position. The person responsible for hiring/firing policies should be required to insure those capabilities are met.

4. Appropriate records, authorization & approval procedures:
   Each transaction should be well documented with receipts, order forms, checks, invoices, etcetera. In other words, some sort of WRITTEN backup that proves exactly what happened. To insure this, each position should have a written job description outlining: title, command chain, general responsibilities, and a description of each duty.

5. Protection of assets:
   The actual assets, as well as the records relating to them, must be protected from loss. A copy of the records should be in a safe place off the business grounds.
6. Monitoring of compliance:
   Last, but certainly not least, the preceding five steps are useless unless someone checks to be sure they are done "by the book".

Part II: Internal Control Problems

Problems Specific to Small Businesses:
If any step mentioned previously is not followed, there is potential risk. Since, due to personnel and financial constraints, it is impossible for a small business to comply with every step of good internal controls, it is imperative the accountant consider certain control issues in light of the characteristics particular to small businesses:

1. Owner/Manager Dominance
   Management involvement can compensate for many weaknesses. However, lack of involvement or over-involvement can create serious problems.
2. Limited Segregation of Duties
   Proper segregation of duties in a small business is usually cost-prohibitive. Even with proper segregation, the informality inherent in a small business often results in departures from procedures.
3. Potential for Management Override of Controls
   Good controls con be totally destroyed by managers and owners who feel they do not need to adhere to their own controls. The attitude of "the assets belong to me" destroys the best internal control system leaving the business vulnerable.
4. Limited Accounting Knowledge of Management
   The tendency of most business manager/owners is to focus on sales, marketing, and product development. There is also an unwillingness to defer judgment to those with superior accounting knowledge out of a fear of "losing control".
5. Inactive or Ineffective Policy Making Body
   Few small businesses have a board of directors to rely upon for guidance. Consequently, most policies are made by the manager/owner, either directly or indirectly, and reflect his/her particular financial weaknesses and preferences.
6. Easy Access to Assets
   Fewer employees increases access to both financial records and physical assets creating opportunities for personal use, theft, and fraud.
7. Lack of Trained Accounting Personnel
   Attempts to "save money" by hiring clerical personnel with 'some bookkeeping' knowledge to perform both clerical and accounting functions increases the probability of errors in the accounting system. Then lack of proper review by a qualified accountant results in misclassifications, duplication of accounts, and total omission of information.
8. Informal Record Systems
   Many small businesses have informal, and improperly designed accounting procedures (usually just a checkbook, and, sometimes, not even that). They also tend to have no idea of the amount of capital that is tied up in inventory and other assets resulting in a business that is "inventory rich" and "cash poor".

Additional Control Problems Created by Computers:

Small businesses are using minicomputers and microcomputers with increasing frequency to process their accounting data using "canned" software which may or may not be adequate for their needs. Automation brings with it certain inherent problems and in the limited environment of the small business, these and other problems are increased.

Problems which are encountered by any automated accounting system user are:

1. Elimination of source documents with records inside the machine.
2. Alteration of information or the system without a trace which allows easy and undetectable falsification of records.
3. Speed & lack of machine judgment causing multiplication of errors.
4. Concentrated information which is easier to steal or lose on a vast scale.
5. User lack of knowledge of the machine and/or its capabilities and/or what the output shoud be which creates an inability to properly check output.

As a result the following list of automation-specific errors can be encountered:

1. Data Entry Error:
   Input entered containing errors
2. Unauthorized Transaction:
   Not properly approved by management
3. Control Level Violation:
   Personnel circumventing controls
4. Lost Transactions:
   Information lost, or rejected by the system
5. Erroneous Output:
   Processing or information error
6. Inadequate Audit Trail:
   Insufficient for reconstruction or tracing of the transaction
7. Cascading of Errors:
   An error in one system will cause problems in another system
8. Improper Cutoff:
   Information placed in wrong month or year
9. Fraud:
   Deliberate plan to remove assets from the business
10. Noncompliance:
    Regulations, policies, or procedures
11. Improper Accounting:
    Not in accordance with GAAP

PART III: IDENTIFICATION AND CONTROL OF AUTOMATED RISK

The only way to control risk is to identify the problem and create a control procedure to prevent it. The following list outlines the steps in this process.

Step 1. Identification of risks- where the loss can occur
Step 2. Determine severity of risk- How much can be lost
Step 3. Determine acceptable risk- How much is too much
Step 4. Identify control points- Where can controls help
Step 5. Develop control solution - what control is needed
Step 6. Cost/Benefit analysis - is it cost effective
Step 7. Implementation - put control into practice

STEP 1: Identification
The easiest way to identify problem areas is to do a review of the business.

General Review:
1. Is a double-entry system of bookkeeping in use and kept current?

2. Does the owner understand and authorize the journal entries, financial statements and required reports?
3. Does the owner use operating budgets and cash projections which are sufficiently informative to highlight abnormalities?
4. Are personal funds segregated from the business?
5. Can the bookkeeping function be performed by another person?
6. Are there adequate safekeeping facilities and retention for records and assets?
7. Are employees handling cash bonded?
8. Is credit approved by the owner and are current credit files maintained?
9. Are sales orders and/or shipping documents approved by the owner and prepared with pre-numbered invoices and memos?
10. Is there a proper cut-off at month's end?
11. Are receivable ledgers balanced and an aging schedule reviewed by management to detect delinquent accounts or irregularities?
12. Are write-offs and other adjustments to customer accounts properly authorized by the owner in writing?
13. Does someone other than the bookkeeper open the mail, prelist all receipts, and stamp the check backs before giving them to the bookkeeper?

Computer Review:
1. Are personnel operating the computer prohibited form custodial &/or authorization duties and programming?
2. Are files and documentation controlled by management with restricted access?
3. Do personnel assignments provide for backup in key positions?
4. Does the system automatically record statistics regarding each job processed and is access to the computer restricted?
5. Do operators & users have to log on and off the computer?
6. Is there a written disaster plan to follow when an interruption to operations occurs and are employees trained in the procedures?
    a. Start up and shut down and restart?
    b. Changes in software or security controls?
    c. Periodic data and program backup protection?
    d. Restoration of data or programs from backup?
7. Are approval initials required on all adjusting or unusual entries?
8. Is responsibility assigned and do adequate procedures exist for tracing and correcting date entry errors?
9. Is the system "user friendly" with easily understood menus and questions to proceed from one process to the next?
10. Is there adequate control and accountability for checks or other negotiable instruments printed by the computer?
11. Are manuals, operating procedures, and systems documents complete and up to date? Are users familiar with manuals provided?
12. Is there a backup system readily available on short notice?
13. Are data files backed up regularly, a log of backup activities maintained and is at least one copy of all backup data and programs stored in an off site location?
14. Is a log of maintenance calls maintained?

STEP 2: Determination of Loss Severity

There are two basic steps for determining the severity of loss:

The first is qualification of the possibility of loss in terms of High, Medium or Low risk.

The following chart provides the basics of this step:

Frequency of Occurrence

Expected Loss		High	Low
	High	Catastrophic	Dangerous
	Low	Important	Immaterial

The second step is to quantify the loss. This may be done in one of four ways

1. Historic Approach:
   Makes projections of possible future losses on the basis of past occurrences. It is a solid method, but its application is limited to risks encountered in the past.
2. Formula Approach:
   This is based on an actual formula derived from the knowledge that risks have two variables: frequency of occurrence and loss per occurrence (see chart above). The expected loss may be calculated as follows:
   Projected Loss = Frequency x Value per occurrence
3. Subjective Estimate Method
   In this method of estimating loss, a specific risk situation is compared to previous experiences with similar situations and arrives at a potential estimate. Its main drawback is its lack of supportability and its subjectivity.
4. Scenario Method:
   This is the least dependable method, but its application may be essential when there is insufficient data for any of the other three. Basically, it draws inferences from similar situations. The main problem is the incompleteness of information in this method.

STEP 3: Determine Acceptable Risk
This is a method whereby the level of risk that may be tolerated is arrived at. It is primarily subjective, but the Quantitative analysis of Step 2 will figure heavily into most decisions in this area. Accountants generally refer to an unacceptable loss quantity as a "material" amount.

This is also an area where a properly prepared budget comes into play. A Properly prepared budget will contain a minimum of:

1. Projected income and expenses
2. Actual income and expenses
3. Detailed analysis of differences both in dollars and percentages

STEP 4: Identifying Control Points
The control points are the same as the risk points. Once it has been determined that a certain area or point of processing contains risk, it becomes a control point in need of a monitoring. If these items are considered in the planning stages and implemented at the same time automation occurs, the cost is minimal compared to altering already established behavior in the company as well as the costs to re-design the system. In order to properly design the system for these items, it is a good idea to :

1. Consult an Accountant with experience in automated systems concerning business. If possible, have him/her go to the computer store to test various systems.

2. Discuss the needs of the business and the Accountant's suggestions with key personnel who will be utilizing the system and get input and suggestions from them.
3. Insure the system is expandable and the software is modifiable at a minimum cost so that it can grow with the business.
4. Purchase from a reliable, established company with a proven record.

STEP 5: Develop a Control Solution

No matter at what point in the design and implementation process the need for a control is identified, the solution to the problem must be designed. This could be as simple as moving the computer to a different room, or as complicated as redesigning the programs to limit user access to sensitive information. Whatever the problem, there needs to be a detailed plan drawn out explaining what is needed, why it is required, and how it is to be accomplished. Again, the process should not be attempted by someone without expertise in the area. Some preliminary suggestions are listed below.

1. Managerial Controls

A system of control built around the manager/owner can substantially compensate for the lack of personnel. Direct supervision by the manager with some of the control duties allocated to him can often produce better Control than more complicated systems. One or two accounting and management courses would by highly recommended for the owner/manager who has not had the benefit of this type training.

2. Review of Timely Reports

Preparation and review of key reports by the owner/manager is an essential control element. His/her close personal knowledge of the operations enhances the effectiveness of this control. Reports that should be included are:

1) Cash and operation statements
2) Sales and production summaries
3) Ratio analysis such as: gross and net profit, inventory and receivables turnovers, industry and liquidity ratios
4) Special control reports such as: aged receivables, inventory analysis, cost analysis, and payables analysis

3. The Budget

Any review of reports is important, but the comparison with a predetermined guideline provides the most effective review. The guideline is the budget which was briefly discussed earlier. A written budget Forces the owner/manager to systematically plan ahead and consider all areas of the business and enables him/her to make a more complete evaluation of the results.

4. Manager Participation in the Accounting Routine

Direct owner/manager involvement in key points include:

1) taking direct charge of the personnel function
2) scrutinizing payroll journals in detail, verifying the net pay column, and signing of all payroll checks
3) being the signing officer with two or more employees required in his/her absence
4) scrutinizing the bank statement before handing them over to the bookkeeper for reconciliation, and/or reconciling the statements personally
5) having sole responsibility for the approval function
6) inspection of all incoming mail prior to receipt by the bookkeeper of data entry personnel
7) other functions to include: reconciling trial balances to the books, review of customer statements prior to mailing, etc.

5. Management Supervision and Staff Competence

The owner can make a contribution to internal controls which cannot be matched by his counterpart in large businesses, and that is his personal observation of the daily operations. A valuable by product is an improved knowledge of the requirements of each job and the character and ability of the employees. It is commonplace for the small business owner or manager to feel that the business "can't afford" the quality of staff required for proper and accurate accounting. It is important to realize that when a large part of the accounting system depends on one , or at the most, two key employees, it is in the interest of the business to insure that they are competent. Well paid capable employees are an investment and make a much greater contribution than a procession of incompetents.

6. Segregation of Duties

the above discussions are not meant to suggest that the division of duties should be overlooked. Personnel not ordinarily regarded as part of the accounting group can be delegated accounting responsibilities. Many primary procedures may be assigned to non accounting personnel such as:

1) bank reconciliations
2) approval functions for sales, purchases, etc.
3) opening and inspection of mail
4) timely deposit and recording of cash receipts
5) check signing and cancellation of support documents
6) verification of receivables to ledgers

7. Mechanical Aids

There are many business machines which save time and increase accuracy and efficiency of personnel while aiding in the control process. These include:

1) Check protectors
2) lock controlled cash registers and invoice writers
3) time clocks, production counters and postage meters
4) one write systems and multiple forms for those functions not performed by the computer
5) Although not mechanical, the use of prenumbered documents can reduce if not eliminate misuse (i.e. invoices, checks, etc.)

STEP 6: Cost-Benefit Analysis

The Corrupt Practices Act of 1977 requires that companies maintain:

"... books, records, and accounts, which ... accurately and fairly reflect the transactions and dispositions of the assets of the issuer ... <and to> ... devise and maintain a system of internal accounting controls sufficient to provide reasonable assurance ... as to the accuracy of the records..."

The term "reasonable assurance" allows for a cost-benefit analysis of controls as part of the evaluation process. Since internal controls are intended to safeguard a company's assets, the costs of the controls should not exceed the potential benefits derived from their use.

The business must determine the cost effectiveness of implementing a particular control. To do this, the following formula may be used:

Amount of loss not realized >= (Potential risk loss + Control cost)

STEP 7: Implementation

Once a problem has been identified, a solution determined and a cost-effective control designed, the final step is the implementation of the control. This does not mean simply putting it to work. It means setting a period of time to train personnel, evaluate the control, make certain it works, and "debug", or finetune it.

Once it is working and running smoothly and all personnel are trained in its use, the procedure should be thoroughly documented and become part of the standard written policies and procedures manual.

CONCLUSION

Internal Controls are the means by which any business protects its assets. Detection and correction of problem areas in control is essential to the success of any buisiness. With the advent of automation, additional opportunities have been created for loss from both ignorance and fraud. A business needs to identify these problem areas, decide the best method to control the problems, design appropriate and cost-effectove controls, and implement them. Without this type of protection, losses can put a business out of business.