

Steps to Prepare for an Audit

Auditing standards have had a major overhaul. That is becoming apparent as letters and articles trickle out of the accounting profession to our clients. Big changes should be expected, but that does little to inform our clients what to do to prepare for the audit. The answer to that question is simple: document the company or organization's internal controls and ensure the most basic and efficient control of reconciliation is implemented. The next logical question is, "What's in it for me?"

A car dealership in the Kalamazoo area closes after allegations of fraud. A Saginaw City Hall worker is accused of embezzling money. A Montrose School District employee is accused of embezzling over one million dollars. An employee of a computer repair store in Ann Arbor is accused of embezzling money. The list goes on and on. From small mom and pop shops to multi-million dollar companies—from non-profits, to governments—fraud and embezzlement are problems. All of the accused were "trusted" employees; only "trusted" employees have enough access to perpetrate fraud. Good internal controls could have prevented these and other frauds or caught them much sooner.

Good internal controls are essential to maintaining accurate financial information. In turn, accurate financial information is essential for making sound business decisions. The best way to make certain that good internal controls are in place is to document what the controls are, review evidence that the controls exist, and periodically review the controls to ensure they are still effective. This means creating an accounting policies and procedures manual.

Creating an accounting policies and procedures manual does not have to be a huge, time-consuming project for one person. If the company or organization has experienced employees, ask them to create an electronic document of how they perform their daily tasks and forward that document to the finance manager for inclusion in the policies and procedures manual. The finance manager or other designated employee can then consolidate the documents into a procedures manual. This also allows the finance manager to ensure employees understand what their responsibilities for internal control are and to review current procedures to see if any updates are necessary. Policies, the entity's position on a given topic, should be included in a separate section of the manual.

The policies and procedures manual will be useful in several ways. Foremost, it will be a training tool for new employees. Many times entities do not have the luxury of an existing employee training a new employee before he or she leaves the company; the policies and procedures manual can aid greatly in the training process. It also clearly dictates whose responsibility internal control is, which in many cases will increase the effectiveness of internal control.

Reconciliations are the easiest and best way to ensure what is being reported in the financial statements is correct. The classic example is a bank reconciliation. Reconcile the difference between what the bank reports and what the financial statements show. Make sure that all deposits recorded were made, all bank fees charged were recorded, no funds were disbursed from the account without being recorded in the financial statements, etc. Many times reconciliation proves that the financial statement amount is not exactly correct. The best time to do a reconciliation is as soon as possible. For bank accounts that means doing monthly reconciliations when the bank statement is received.

All balance sheet accounts should be reconciled to some type of supporting data. Accounts receivable should be reconciled to aged receivable reports that are periodically reviewed for accuracy and collectibility. Accounts payable should be reconciled to aged payable reports and reviewed to ensure all payables are recorded. Fixed assets should be reconciled to the current

or prior year depreciation schedules and reviewed to ensure all purchases over the capitalization threshold are recorded in fixed assets and not expensed.

What if there is not enough time to reconcile all of the balance sheet accounts? Reconcile the riskiest accounts first. In general, checking and cash accounts will be the riskiest because cash is a desirable asset to be stolen and checking accounts have large quantities of transactions. Rate the other accounts according to risk. A high volume of transactions, a large dollar value of transactions, or a high dollar account balance are all quantitative risk factors that lead to a higher risk. Qualitative factors should also be considered such as the complexity of transactions, fraud susceptibility, subjectivity of accounting rules, etc. High risk accounts need to be reconciled on a monthly or quarterly basis. Low risk accounts may not be reconciled on a regular basis but should have analytical procedures applied to them on a routine basis. Analytical procedures include comparing this year to last year, actual to budget, or actual to expectations. If something varies dramatically, do a reconciliation.

Monitoring procedures are the most important aspect of internal control. Without monitoring, there is no incentive for employees to follow documented procedures and no checks and balances to guarantee those procedures are followed. Monitoring includes reviewing the output from various systems (such as reviewing financial statements). It also includes reperforming procedures periodically and reviewing documentation that procedures have been performed.

All of these procedures can help ensure the monthly financial statements used for making important financial decisions are correct. Reconciliations done on a timely basis are a good control procedure for ensuring accurate information is recorded on the balance sheet. Although the policies and procedures manual may take some time to create, it will help in the long run to train new employees and to expose activities for which new control procedures need to be implemented. All of these procedures will help reduce the risk of fraud. In addition, they will aid the auditor in meeting the new audit standards.

Policies and Procedures to Document

Different entities need to document different policies and procedures. The following list of policies and procedures is not inclusive, but they are common for most entities and a good place to start.

Area	Policies and Procedures to Document
Accounts Receivable and Cash Receipts Procedures	• handling money
	• receipting cash
	• accessing cash registers, including who can access them
	• keeping money, including where it is kept
	• depositing money
	• granting credit
	• recording accounts receivable
	• collecting receivables
	• preparing the bank reconciliation
	• reviewing reconciliations, including what to look for in the process
Accounts Payable and Disbursement Procedures	• monitoring
	• handling invoices
	• authorizing purchases, including who can authorize
	• noting the time during the month when bills get paid
	• authorizing payments, including who can authorize

	<ul style="list-style-type: none"> entering the bills into the computer system and posting to the general ledger
	<ul style="list-style-type: none"> accessing checks, including who can access them
	<ul style="list-style-type: none"> recording year-end accounts payable
	<ul style="list-style-type: none"> monitoring
Payroll Procedures	<ul style="list-style-type: none"> handling new hire information
	<ul style="list-style-type: none"> handling employee terminations
	<ul style="list-style-type: none"> determining employee versus independent contractor status
	<ul style="list-style-type: none"> determining pay dates (weekly, bi-weekly, semi-monthly)
	<ul style="list-style-type: none"> paying different types of employees (salary, hourly, etc.)
	<ul style="list-style-type: none"> handling overtime, vacation, sick, and disability pay
	<ul style="list-style-type: none"> calculating withholdings
	<ul style="list-style-type: none"> distributing checks
	<ul style="list-style-type: none"> calculating compensated absences
	<ul style="list-style-type: none"> accruing year-end amounts
	<ul style="list-style-type: none"> monitoring
Journal Entry Procedures	<ul style="list-style-type: none"> preparing and approving journal entries
	<ul style="list-style-type: none"> requiring internal forms
	<ul style="list-style-type: none"> storing supporting information, including the location, form, and content
	<ul style="list-style-type: none"> monitoring
Fixed Asset Procedures	<ul style="list-style-type: none"> determining capitalization limits
	<ul style="list-style-type: none"> determining useful lives
	<ul style="list-style-type: none"> disposing of equipment
	<ul style="list-style-type: none"> maintaining a schedule of fixed assets and depreciation
	<ul style="list-style-type: none"> monitoring
Estimate Procedures	<ul style="list-style-type: none"> preparing and approving estimates, including who is authorized to do so
	<ul style="list-style-type: none"> requiring documentation to support estimates
	<ul style="list-style-type: none"> calculating and preparing annual estimates such as the allowance for doubtful accounts
	<ul style="list-style-type: none"> monitoring
Monthly Financial Statement Procedures	<ul style="list-style-type: none"> preparing monthly financial statements
	<ul style="list-style-type: none"> formatting monthly financial statements
	<ul style="list-style-type: none"> determining what basis of accounting to use
	<ul style="list-style-type: none"> creating due dates for monthly financial statements
	<ul style="list-style-type: none"> distributing reports, including who should receive them
	<ul style="list-style-type: none"> reviewing monthly financial statements
	<ul style="list-style-type: none"> monitoring
Computer Security Procedures	<ul style="list-style-type: none"> determining access controls
	<ul style="list-style-type: none"> authorizing use
	<ul style="list-style-type: none"> authorizing new programs and changes to existing programs
	<ul style="list-style-type: none"> using the Internet
	<ul style="list-style-type: none"> planning for disaster recovery
	<ul style="list-style-type: none"> planning for contingencies
	<ul style="list-style-type: none"> backing up files
	<ul style="list-style-type: none"> testing of backup files
	<ul style="list-style-type: none"> storing of backup files
	<ul style="list-style-type: none"> scanning for viruses
	<ul style="list-style-type: none"> creating and maintaining firewalls
	<ul style="list-style-type: none"> monitoring

