How to Save Your Organization $147,000

Preventing fraud in your organization

COUGARMOUNTAIN

ACCOUNTING SOFTWARE FOR GROWING BUSINESSES

Table of Content

Who will benefit from this eBook?

This paper is intended for business owners, nonprofit executives and leaders, bookkeepers, office managers, or anyone else responsible for the integrity of their organization and the financial systems that are being used.

Introduction

What comes to mind when you hear the term “fraud?” Enron? Bernie Madoff? It’s likely to be complicated schemes swindling millions from Fortune 500 companies and not a small company like yours, built on strong relationships and honest practices. While it may not make national news, smaller businesses are both more likely to be affected by occupational fraud and suffer greater losses than large companies. According to a study of 1,388 fraud cases by the Association of Certified Fraud Examiners (ACFE), more than 30% occurred in businesses of fewer than 100 employees, with a median loss of $147,000. Can your company afford a loss like that?

In small organizations, it is harder to divide work processes among more than a few people. Because of their size, these same small businesses are less likely to have procedures for sound internal oversight. The result is that fraudsters can more easily begin schemes and keep them going for longer. Too often, owners and managers rely on personal trust in place of documented policies, periodic reviews, and thorough record keeping. But trust alone isn’t enough to safeguard against fraud before it happens. As the old saying goes: Trust, but verify.

This eBook identifies and discusses five kinds of schemes that commonly threaten smaller businesses: payroll, purchasing, expense reimbursement, cash receipt, and hiring. All of these except hiring fraud are *asset misappropriation* schemes, which involve direct embezzlement of resources and revenue.

Five Common Types of Fraud

Payroll Fraud

Payroll fraud schemes involve exploiting the compensation process. Exaggerating work hours, reporting false overtime, inflating pay rates, and writing checks to fictitious employees are common examples of this kind of embezzlement, which on average goes undetected for three years.

Purchasing Fraud

Purchasing fraud involves manipulating deals with outside vendors and, on average, is one of the most costly embezzlement schemes. Common schemes include cutting favorable deals for cash kickbacks and setting up shell vendors to funnel funds into an employee’s pocket.

Expense Reimbursement Fraud

Expense reimbursement fraud involves exaggerating or inventing business expense reports. Schemes range from an exaggerated taxi fare to entire luxury vacations written off on the company dime. This is one of the most common types of workplace fraud and often starts small, but grows over time.

Cash Receipt Fraud

Embezzlement of cash receipts comes through *skimming* (stealing money before it is recorded in the company books) or *larceny* (stealing money that has been recorded—usually before it is deposited in the bank). Charities, ministries and other nonprofit organizations that deal in small donations are particularly at risk for this kind of fraud.

Hiring Fraud

Someone may exaggerate or invent credentials and experience to get hired, leaving a business with an employee who is both unqualified and morally questionable. This is one of the easiest forms of workplace deception and one of the toughest to spot.

Payroll Fraud

Small organizations are more likely to have few, if any, documented and implemented internal controls. Payroll fraud occurs nearly twice as often in small organizations as in large ones and usually goes undiscovered longer than any other type of fraud, lasting on average 36 months, reports the ACFE. A payroll manager at the Brooklyn Museum embezzled $620,000 by wiring 38 checks to fictitious employees. His would-be workers were named “Brooklyn,” “Brooklyn Museum,” and “ZXY,” yet the scam went undetected for three years!

Common schemes of this type include:

- Entering non-existent “ghost” employees into the system and then paying them
- Continuing to pay former employees after they leave the company
- Forging or duplicating pay rate changes, commissions, and bonuses
- Adding extra hours to time records and reporting false overtime

Strengthen the payroll process with independent review

Periodic review and tests, preferably by an independent reviewer or accountant, is the best internal control against payroll embezzlement for small companies where it is difficult to separate duties among three or more people. This type of oversight reduces losses by almost 60% and the length of fraud schemes by over 40%, according to the ACFE.

A review does not need to occur every month; this type of oversight is most effective when the employees that process payroll don’t know when the reviewer is coming, what periods will be reviewed, or what tests will be performed. An independent reviewer should perform these 10 tests:

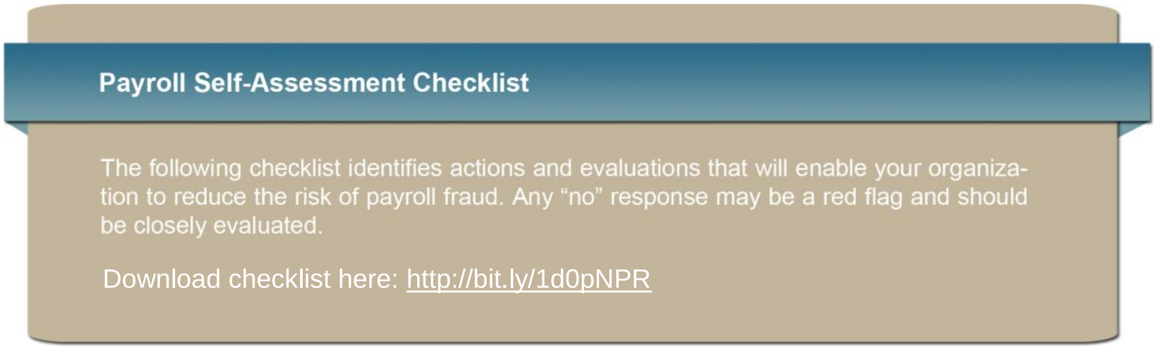
1. Verify that each employee who received a check (1) existed and (2) was employed during the period.
2. Verify that the final paycheck made to a terminated employee was correct and that no further paychecks were issued. Continuing to pay former employees is a common scheme.
3. Match the addresses on checks or employee files to employee addresses. If more than one check is going to the same address, it could be a ghost employee.
4. Verify that pay rate changes, bonuses, commissions, and the like were properly authorized, documented, calculated, and paid.

Internal controls protect both the company and its employees

A tight, documented system of internal checks and balances is just as important for a smaller organization as a large one to stop payroll embezzlement. The presence of strong internal controls does not imply suspicion of accountants, bookkeepers, and managers. Rather, these controls are evidence of a well-run organization whose leaders are committed to integrity, transparency, and professionalism. Furthermore, in addition to uncovering dishonest acts, a documented system of checks and balances can help spot honest errors.

5. Verify that any time records were signed by each employee, properly approved, and recorded correctly in the payroll system.
6. Verify that bank reported direct deposit amounts match those in the payroll system.
7. Review payroll tax withholdings and filings for proper calculation and timely payment.
8. Match the payroll register to the supporting documents.
9. Develop trend reports of overtime to determine if there is abuse. Padding hours is one of the most common types of abuse.
10. Verify that supervisors are properly approving employee time cards.

It isn’t necessary to perform every test every month. It is a strong deterrent if the people who process payroll know someone will be conducting these types of tests, but don’t know what periods will be tested or when the testing will be done.



Payroll Self-Assessment Checklist

The following checklist identifies actions and evaluations that will enable your organization to reduce the risk of payroll fraud. Any “no” response may be a red flag and should be closely evaluated.

Download checklist here: http://bit.ly/1d0pNPR

Purchasing Fraud

For an employee that does business with outside vendors, it can be easy to cut favorable deals for bribes or cash kickbacks, skim money off the top of a transaction, or even set up a shell organization to funnel money out of the company and into their pocket. The Association of Certified Fraud Examiners reports that the median loss for purchasing fraud in 2012 was $200,000, and the risk is even higher for smaller companies that have only a few employees in charge of purchasing and billing.

Any outside contract, for example, between an equipment supplier and an office cleaning service, can play host to purchasing fraud schemes, which most commonly fall into these categories:

- *Fictitious vendor* schemes, in which an employee sets up and processes invoices to a false vendor.
- *Vendor Kickbacks* can encourage employees to go against company interests. Employees may sell a favorable contract in exchange for expensive gifts and five-star treatment, or just accept cash under-the-table.
- *Conflicts of Interest* occur when a purchaser channels business to a company in which he, his family, or his friends have a financial interest.
- *Bid Rigging* is common on large projects with several competitive bids, often with doctored bid documents that contain unnecessarily restrictive requirements designed to channel a bid to a specific vendor.

How to report fraud

Tipoffs account for more than 40% of all asset fraud detection, often through an anti-fraud hotline. Always provide ways to report unsafe and unscrupulous activity anonymously and without fear of retribution. Promote the reporting methods to vendors, donors, and other stakeholders, so you hear about inappropriate activity and can take action before the media and your donors hear about it.

Strong safeguards against purchasing fraud incorporate these three factors: employee **accountability**, **segregation of duties,** and vendor **analysis**.

Accountability in the workplace

Safeguarding against purchasing fraud begins with a clearly stated and documented conflict of interest policy that gives examples of what are acceptable and unacceptable gifts from vendors. Also consider having employees that purchase for your business complete and sign an annual conflict of interest questionnaire.

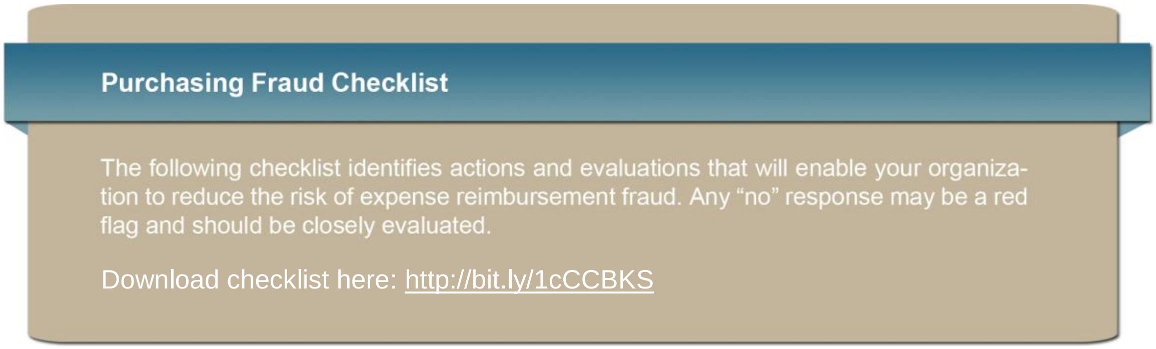
Segregation of duties

A business is most vulnerable to purchasing fraud when one person has too much power over contracts, receiving, and paying or approving vendor payments. Separate those functions as much as possible. For example, additions and changes to the master vendor file should be made by someone who is independent of the cash disbursement process. Perform a three-way match of the receiver/packing slip, purchase order, and invoice before you pay any vendor. If your organization does not use purchase orders, make sure each purchase has been authorized and the authorization is documented.

Tools of analysis: Know who you're paying

A good practice is to periodically analyze your vendor file and payment invoices. Here are some tips to make sure vendors exist and are honest and legitimate:

- Compare the amount paid to each vendor and types of vendors over time—at least annually—and look for multi-year patterns.
- Review the vendor file periodically for the use of acronyms in a vendor name, PO Box addresses, and physical addresses.
- Cross reference addresses and phone numbers to the employee payroll file; a match might indicate a fictitious vendor. Often, the vendor name is similar to a legitimate vendor, or a new vendor is set up using the acronym of a legitimate vendor (e.g., Big City Plumbing, Inc. becomes BCPI).
- Always check for duplicate invoices from the same vendor.



Purchasing Fraud Checklist

The following checklist identifies actions and evaluations that will enable your organization to reduce the risk of expense reimbursement fraud. Any "no" response may be a red flag and should be closely evaluated.

Download checklist here: http://bit.ly/1cCCBKS

Expense Reimbursement Fraud

Employees who exaggerate or falsify their business expenses often tell themselves that there is nothing wrong with padding a mileage report, double dipping on travel expenses, or taking a well-deserved vacation on the company's dime. They choose to perceive it as a victimless crime that everybody commits. While it often starts small, this kind of embezzlement tends to grow over time and can be seriously costly. The ACFE reports that expense reimbursement frauds result in a median loss of $26,000 per incident and represent 14.5% of all employee fraud. Common expense reimbursement schemes include:

- Getting extra receipts from an accommodating cab driver
- Recording tips that were never paid
- Getting duplicate receipts at hotels and restaurants
- Double-billing for plane tickets and rental cars
- Getting a massage or facial after a long day at a conference
- Having a family dinner at a nice restaurant characterized as a business development expense
- Changing a 1 to a 7, or a 3 to an 8 on a receipt
- Getting reimbursed for some items, then selling them on e-Bay

The most effective way to prevent or quickly detect expense reimbursement fraud is a balanced approach of **prevention**, **detection**, and **enforcement**.

Prevention

An expense reimbursement policy is the first step towards fraud prevention. The policy should include clear definitions of allowable expenses, how expenses are reviewed and reimbursed, and the process for submission. The policy helps prevent or limit fraud impact by clearly stating the rules related to approvals, limits, amounts, supporting documentation, and requirements for

Responding to fraud

In responding to a potential fraud situation, fact-finding is an essential first step. Consider these questions: How much is involved? Is it the first time the individual has exaggerated their expenses? If not, how long has it been occurring? Is this limited to one person? One department? Or is it throughout the organization?

Once the facts have been gathered, move to action. Sit down with the employee with the defined purpose of obtaining more information and educating the offender about expectations and potential consequences:

1. Clearly set objectives before the meeting.

2. Open the meeting by setting expectations. For example, "I noticed some questionable expenses in your last three expense reports and would like to better understand this pattern."

3. Actively Listen. Ask open-ended questions and then listen carefully to the responses. Be cautious about making accusations.

4. Educate the person about your organization's values, expectations, and policies.

5. Establish a follow-up plan. Be direct and to-the-point.

6. Document the discussion and any follow up activities.

receipts. Everyone in the organization should be educated about expenses and the expectation of ethical use of the reimbursement policy.

Be sure to develop a procedure for handling the gray areas where rigid rules don’t work. There will always be a few of these, so be prepared. Communicate the policy to employees at all levels, and provide managers and supervisors with training on how to identify unusual activity. Management’s support of and adherence to the spirit and letter of the policy is key to ensure compliance throughout the organization.

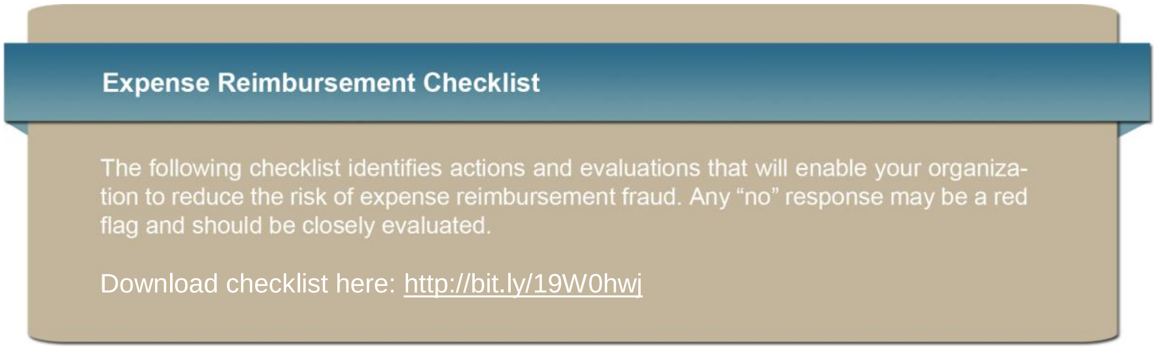
Detection

Many managers don’t have, or take the time, to thoroughly scrutinize expense reports, so they approve whatever purchase has a receipt attached. Employees know this and exploit lax oversight. Train managers to examine expense reports closely and watch for these red flags:

- Expenses that are significantly over budget compared to prior years
- Expenses claimed on dates/times the employee was not working
- Expense amounts just under the threshold for review or requirement of a receipt
- Minimal or non-existent supporting documents
- Photocopy of receipt rather than original receipt
- Sequential receipts
- Expense reports approved by someone outside the employee’s department
- Unusual or excessive reimbursement to one employee. For example, two sales people with the same position, where one has monthly expenses of $8,000 and the other’s is $1,000.

The “trust, but verify” review process is a good rule of thumb here. Make sure employees know someone familiar with their responsibilities will review and approve expense reports, and an independent reviewer should scrutinize a sample of reports periodically. The reviewer should ask questions of employees and help train managers to be savvy approvers. To encourage compliance, make sure employees know someone other than immediate supervisors will scrutinize their reports.

Expense reimbursement fraud should always be addressed, whether the item in question is a duplicate taxi fare from the newest sales rep or a five-star hotel for the CFO. Ignoring the problem is tacit approval, which will only encourage further embezzlement.



Expense Reimbursement Checklist

The following checklist identifies actions and evaluations that will enable your organization to reduce the risk of expense reimbursement fraud. Any “no” response may be a red flag and should be closely evaluated.

Download checklist here: http://bit.ly/19W0hwj

Cash Receipt Fraud

Cash skimming (stealing receipts before they are recorded) and cash larceny (stealing receipts that have been recorded in the books) accounted for 1 in 5 cases of embezzlements of $100,000 or more, second only to forging checks, according to the 2011 Marquet Report on Embezzlement. It was also responsible for one quarter of all workplace fraud cases studied by the ACFE in 2012. Cash receipt fraud includes stealing checks that are easy to convert to cash. This kind of fraud is a serious danger to small companies that have one or two employees handling cash and personal checks. Cash skimming and larceny are twice as likely to affect organizations with fewer than 100 employees.

Cash embezzlement can be especially easy to commit in nonprofit organizations that deal in donations: In 2012, it accounted for 40% of all fraud in religious organizations, charities, and social services, reports the ACFE. Ironically, churches that operate with a high level of trust are some of the most frequent victims. In 2006 Richard and Philip Cunningham, father-son ex-pastors of a Baptist church in California, allegedly stole $3.7 million using a variety of schemes over three decades. Between them, they owned luxury cars, six homes, and two timeshares—all on salaries supposedly less than $100,000/year.

Internal review to protect and maintain honest business

As with payroll fraud, in small organizations where it is difficult to separate duties among three or more people, the best internal control is periodic review and tests, preferably by an outside accountant. It doesn’t need to be done every month. This type of oversight is most effective when bookkeepers know that someone will review their work in detail, but they don’t know when the reviewer is coming or what periods will be reviewed. And even if there is no intentional fraud, thorough reviews can help tighten up the revenue cycle by spotting honest mistakes.

No good deed goes unpunished: Preventing cash receipt fraud in nonprofit organizations

It’s a simple thing for donations to vanish from the coffer before they go on record, or for a few checks to go missing after a fundraiser. These four questions can help nonprofit organizations protect staff and volunteers from the temptation of an open coffer.

1. *Is the organization being safe from the start?*

Take steps to minimize risk of a revenue theft scheme before money hits the door. Have more than one person receive the mail or pick up donations. Two people working together should count the funds, endorse checks, and create a detailed audit trail *before* the funds are taken to the bank. The people who count the money and prepare the deposit should not have access to the accounting system or the donor database. Even small organizations should be able to separate these functions by creative use of receptionists and other staff/volunteers.

2. *Are adequate records maintained?*

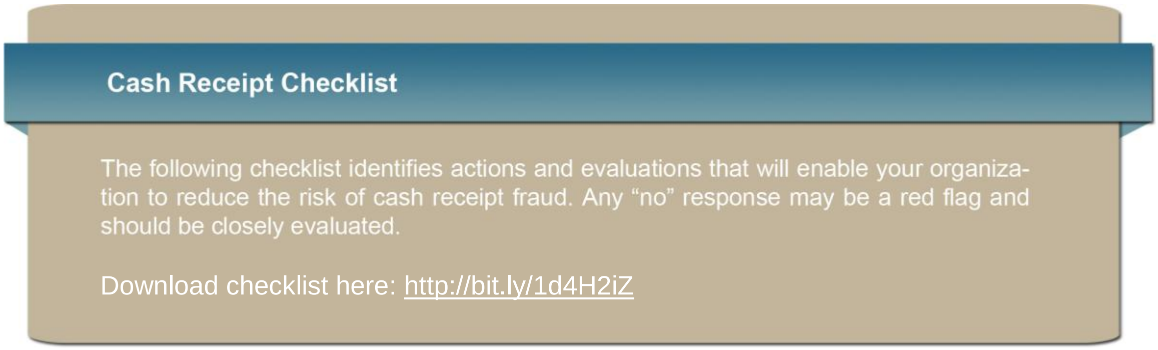
Retain a copy of the audit trail for the independent reviewer. It can be used to compare to cancelled deposit tickets, financial statement revenue, and the accounts receivable system or donor database.

3. *Is the organization acting promptly?*

The longer money lies around, the greater the risk of theft. Deposit funds immediately, the same day they are received. Consider a “remote deposit capture” system available from banks and software vendors so checks can be deposited without going to the bank.

4. *Are fundraising events staffed properly?*

Make sure you have controls in place at fundraising events so that cash doesn’t disappear on the way back to the office. Have people counting in groups of three——two to count, recount, and document each batch, and a third person to observe.



Cash Receipt Checklist

The following checklist identifies actions and evaluations that will enable your organization to reduce the risk of cash receipt fraud. Any “no” response may be a red flag and should be closely evaluated.

Download checklist here: http://bit.ly/1d4H2iZ

Fraud at the Hiring Level

A few months before it was discovered she lied about her credentials, former MIT admissions dean Marlee Jones had received the institution’s highest administrative award and was on tour to promote her co-written book on personal achievement called “Less Stress, More Success.” To get her MIT job, she listed multiple degrees and even a doctorate, but it turned out, Jones didn’t even graduate from college.

Research is divided on the frequency of hiring fraud; one study by the American Psychological Association found misrepresentations in 67% of the resumes of job applicants in the United States. Other studies place the number between 20% and 70%, but that means that even under the smallest estimate, one in five resumes contain embellishments, omissions, and intentional inaccuracies. Of course, not all of these are as major as listing a bogus doctorate, but small omissions and embellishments can indicate a lack of integrity and tendency to cut corners that can become a serious problem for the company later on, or at least, keep the position from the most qualified candidates.

Leaders can avoid unwittingly making bad hires by taking steps to initially **analyze** a prospective employee’s claims and then to **verify** the candidates experience and credentials.

Analyze: Watch for resume red flags

Even deceivers can seem trustworthy; hiring personnel should always be skeptical and suspicious when reviewing a resume and other credentials. Keep an eye out for signs of these warning signs:

- *Suspicious dates:* A prospective employee can stretch dates to cover up a long stint of unemployment or jail time, or to omit an episode of past employment where they left in unfavorable circumstances (perhaps they were caught lying on a resume).

- *Inflated Claims:* Most fraudulent credentials aren’t totally made up, just inflated and exaggerated. These include advanced degrees and military and community service. It is also a simple matter to alter job titles and puff up listed responsibilities.

- *Made-up Credentials:* False degrees, unearned positions, and invented awards. Worse, advanced software and printers can make fabricating official-looking documents a cinch.

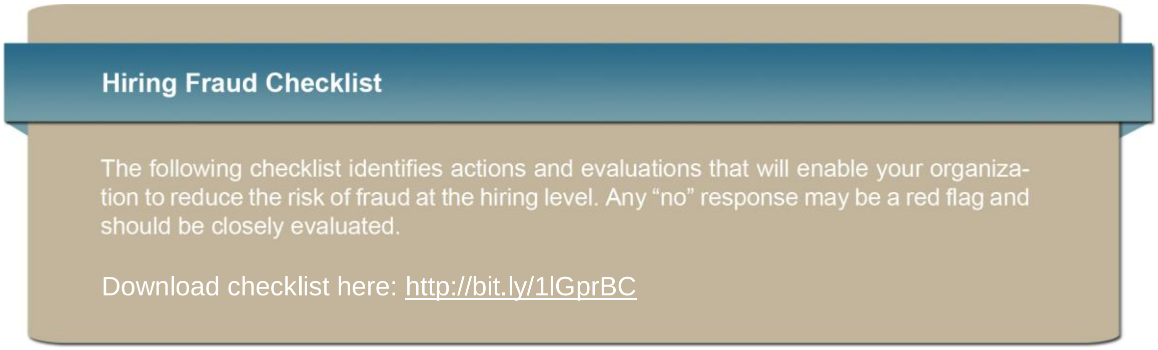
- *Vagueness:* Lack of details can be attempts to mask lack of experience. For example, “ten years in the financial service industry” could describe the janitor of the local credit union.

- *Bogus References:* An ambitious employee may enlist a cohort to play the part of past employer, and some websites will fabricate glowing references for a relatively small fee.

Verify:

The resume looks sound and the credentials seem legitimate, but that may only mean the candidate is a good bluffer. An employer should always take steps to verify a candidate's claims before they make a job offer.

- At minimum, make every offer of employment contingent on the results of a background check.
- For finance positions, consider adding a credit check. Do a credit check at hire and every couple of years thereafter. Financial stress is one of the key risk factors for embezzlement and fraud. Do you want someone managing your organization's finances if they can't manage their own?
- Check credentials online using state licensing body websites for anyone who claims to hold a license, even if it is not relevant to the position.
- Check the National Student Clearinghouse for college and university degrees and the National Sex Offender registry database, especially if your organization services children or the elderly.
- Call references, but not necessarily the ones the candidate provides. Ask open ended questions and compare the responses to claims on the candidate's resume and from in-person interviews.
- Do the same checks on temporary employees, even if they come through an agency.
- Establish a "no tolerance" policy with job candidates as well as established employees. This sends a strong message that your company values character and integrity.
- Always consult an employment law attorney before adopting new policies.



Hiring Fraud Checklist

The following checklist identifies actions and evaluations that will enable your organization to reduce the risk of fraud at the hiring level. Any "no" response may be a red flag and should be closely evaluated.

Download checklist here: http://bit.ly/1lGprBC

Creating an Audit Trail with Cougar Mountain Software's DENALI Solution

An audit trail is a chronological record of all your transactions, and it is a vital record for any business to maintain. A strong audit trail provides the ability to monitor all activity for fraud, find and enter lost transactions, and supply ready documentation for internal and external audits, including a government audit.

An audit trail is especially important for nonprofit organizations which generally deal with more scrutiny from outside organizations. Having detailed records for all donations and the ability to show how the money was used can be invaluable when a government agent is breathing down your neck asking about expenses.

Although this might sound daunting, you can rest easy when you use Cougar Mountain Software's DENALI accounting solution, which has features to help you implement and preserve your audit trail in these crucial areas:

- Business controls
- Transaction monitoring
- Reporting

The DENALI Controller module helps you implement business controls. Setting security for each user specific to every window in the software allows managers to control who has access to certain modules or features within the modules. You won't have to worry about unauthorized access to financial records or data because you can simply set security rights to disallow access to those areas of the program.

DENALI provides several reports that allow you to track transactions from start to finish.

The DENALI Audit Trail Report can show you details of every transaction that was posted to General Ledger, which allows you to quickly and efficiently monitor transactions. You can also print a History Report from each module that shows you every posted transaction, in detail, with filters that can show only what items you want to see in the order you want to see them.

The breadth of DENALI's audit trail lets you focus on other areas of your organization and track every transaction from source to completion. Although protecting your organization from fraud can feel overwhelming, DENALI gives you plenty of security options to keep your data files and financial records safe.

For More Information

For more information on protecting your business with audit trails visit:

www.cougarmtn.com

Appendix: Further Resources

Please consult these additional resources for more information about the impact and prevention of fraud and embezzlement.

Association of Certified Fraud Examiners
www.acfe.com

Association for Financial Professionals
www.afponline.org/fraud

Find a CFE Directory
www.nf.acfe.com

National Association of Forensic Accountants
www.nafanet.com

The 10 Worst Corporate Accounting Scandals of All Time
www.businesspundit.com

The Federal Bureau of Investigation
www.fbi.govs/scams-safety

The U.S. Small Business Administration
www.sba.gov

Credits

Denise McClure, CPA, CFE – Owner Averti Solutions

Denise McClure brings over 20 years of experience in public accounting, business management, and nonprofit board involvement to her work as a Certified Public Accountant (CPA) and Certified Fraud Examiner (CFE). Her business, Averti Solutions helps businesses and nonprofit organizations become more profitable, secure, and efficient by creating accountable and transparent work environments.

http://www.avertisolutions.com
Denise@AvertiSolutions.com

Averti Solutions, LLC
1533 N Milwaukee Avenue, #181
Boise, ID 83704

Phone: (208) 989-2245

Cougar Mountain Software

Cougar Mountain Software was founded in 1982 with a vision to develop powerful business accounting, nonprofit accounting, and point of sale software solutions (read the Cougar Mountain Story). Our 30 years of success comes from two key practices; (1) employing in-house accounting and business professionals for our sales, support, training, and development teams, and (2) listening to our clients. These two practices make our accounting solutions unique to competitors who outsource their support and build fixed and un-scalable solutions to meet the general needs of the masses.

www.cougarmtn.com

Cougar Mountain Software
7180 Potomac Dr.
Boise, ID 83704

Phone: (208) 375-4455
Fax: (208) 375-4460