

Miriam Robeson

(website) www.lawlatte.com

(email) lawlady1@gmail.com

Sales Tax Compliance - Sales

- ALL SALES
 - Sales of inventory or product for sale more than 30 days in a year
 - 30 "Sale Days" do not have to be consecutive to trigger sales tax collection rule
- NONPROFIT – may be exempt from paying sales tax, but must report sales and exempt sales.

What do you do if you get a tax letter?

- Tax Notice Letter
 - Federal
 - State
- DO NOT IGNORE!
 - Frequently – just need updated information
 - Incorrect designation of tax payment (employment, sales)
- 1st Letter – Demand Notice
- 2nd Letter – Tax Warrant – SHORT TIME FRAME!!
- 3rd Letter – Tax Lien

Handout – 10 Tips for Keeping an Eye on Finances

Financial Oversight

Watch the money – Watch the people

Financial Oversight is the review of both finances and financial practices

Ensures safe, ethical financial procedures

Protects the Company and the Directors/Staff

Provides integrity and transparency to the public

Catches financial difficulties before they become financial impossibilities

Handout - Nonprofit Financial Control Policy

Accountability -
Financial Governance Policies

- Policies for –
 - Handling Money
 - Recording Money
 - Reporting Money

Handout - Document Destruction Policy

Accountability
Financial Controls

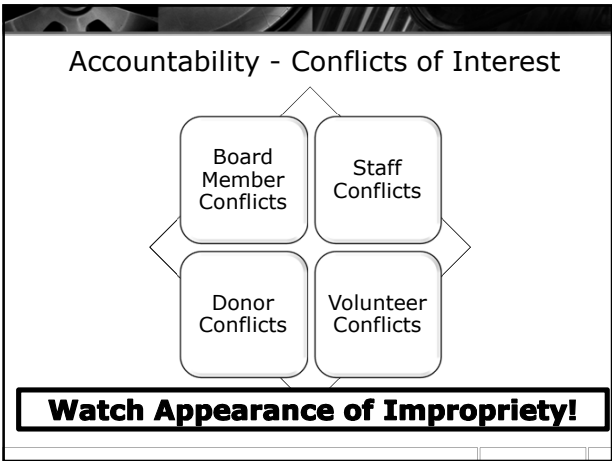
- GAAP Standards
- Financial Procedures Manual
- Restrictions documented and honored
- Training program for Staff and Board
- Document Retention/Destruction Policy

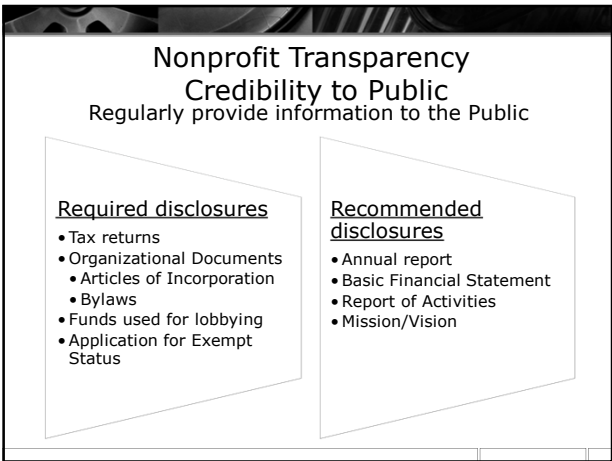
Handout - Conflict of Interest Policy

Accountability - Governance

Conflict of Interest

Ethical Standards







Risk Management Plan Handout - Risk Management Policy

Types of Risk to Manage

- People**
 - Board members, volunteers, employees, clients, donors, the public.
- Property**
 - Buildings, facilities, equipment, materials, copyrights, trademarks
- Income**
 - Sales, grants, contributions, sponsors, fund raising
- Goodwill**
 - Reputation, stature in community, ability to raise funds and appeal to prospective volunteers

Handouts - 10 Ways to Catch Fraud and Mistakes from Outside
Handout - 15 Ways to Minimize Employee Fraud

Risk Management - People

- Poor economy has resulted in an increase in criminal conduct against nonprofits
- Embezzlement by employees
- Embezzlement by officers
- Fraud from "outsiders"

- Phrase of the Day - "Trust But Verify"

Fraud --
What to do when it happens to you!

Fraud in the Corporate Sector

- Upper management commits 18% of fraud
- Accounting Department commits 29% of fraud
- (Source: Association of Certified Fraud Examiners)

Top mistakes made in response to fraud

- Fear-based (or other emotional) response
- Letting the perpetrator "off the hook"
- Assuming that the bank (or other organization) will "handle it"

Fraud Alert!

Fraud -- What to do when it happens to you!

If you suspect fraud - act immediately!

- Lock-down data
- Start a formal audit process with outside auditor
- Change procedures and rotate staff responsibilities

If you verify fraud

- All of the above, PLUS
- Confront the perpetrator (employee, officer, outside contractor)
- Copy and compile evidence in a separate, protected and confidential file
- Contact the police, if appropriate

Handout - Someone Stole the Cashbox!

PR for Nonprofits Public Relations During Fraud Crisis

If Fraud or embezzlement finds your Nonprofit.

- How the public hears about and perceives the incident can drastically affect the nonprofit's ability to move beyond the event.

DO NOT HIDE or Minimize the seriousness of the event

- If you are contacted by the press, answer! - if you don't get your story out, no one will, and speculation will replace facts

Have a plan of action for response

- If employee: suspension, termination
- If board member: resignation, removal
- Note appearance of impropriety is enough to take action for a board member, but more evidence is needed to take action against an employee

Handout - Public Relations in Times of Crisis

Preventing Fraud

Have and use financial control policies

Know who handles the money

Remove temptation

Review financial information

- ALSO - have independent review of finances

Be aware that it can happen YOU!

Keeping on the Right (Financial) Path



Any Questions?
Thank you for your attention!

Miriam Robeson, Attorney

Today's materials are available on
Miriam's Website:

[http://blog.lawlatte.com/index.php
/upcoming-workshops/](http://blog.lawlatte.com/index.php/upcoming-workshops/)



Top 10 Small-Business Tax Audit Triggers

1. **Hide income.** If you get paid in cash, rather than by check or credit card, it's tempting to just 'forget' to declare some of that income. That's a huge IRS no-no. Remember that the income you don't declare might be the deduction someone else takes. Particularly with 1099-MISC income, the IRS computers are getting better at matching YOUR income with some else's expenses.
2. **Make more than a million dollars.** Have an adjusted gross income of more than a million dollars? You'll have the highest chance of getting audited. In 2008, according to the IRS, they audited 5.6% of millionaires' returns, compared with 2.9% of those making more than \$200,000, and less than 1% of those making less than \$200,000.
3. **Mix personal and business expenses.** Be reasonable in deducting "personal" expense. If it's only an incidental business use, don't take it as a deduction, particularly if it "looks" personal (like a trip to an exotic local, or the purchase of a home furniture item that doesn't look office-related).
4. **Entertainment Expenses.** Another area where personal and business expenses are likely to be construed as intertwined. Remember, you can only take 50% of entertaining and food expenses as a deduction. Nevertheless, small businesses need to be out there talking to customers over lunch or dinner, at a ball game or golfing. Most entrepreneurs don't entertain nearly enough. Do.
5. **Lose money more than three out of five years (Hobby-loss Rules).** The IRS is on the lookout for people writing off hobbies as businesses (so forget buying those expensive cameras and calling yourself a pro photographer). They want to see that you've at least had the intent to make a profit. Don't.
6. **File a Schedule C return.** If you're a sole proprietor, you'll file a Schedule "C" — Profit or Loss from a Business — as part of your 1040 form. If you use a Schedule C, make sure you have proper documentation. Consider forming an LLC or Corporation as your business identity.
7. **Take the home office deduction.** If you work at home, remember you need a section of your house exclusively used for business to qualify for a home office deduction. Be careful that you do not abuse this benefit by taking "too much" as a home-office deduction.
8. **Use your car for business.** Like entertaining, this is another area the IRS thinks has the possibility of being misused. You're less likely to be audited if you have a separate business car, but not everyone can afford that luxury. Keep good travel records. 2010 mileage rate was 50¢ – 2011 mileage rate is 51¢.
9. **Don't E-file.** The IRS would like to see everyone use E-file for your tax return. It's more accurate for the IRS and more likely to find errors for your (sometimes errors that are in your favor). Hand-coded paper returns may reveal more errors that are followed up with an IRS audit letter.
10. **Deduct Unreasonable Expenses.** The IRS has a database of industries, including expected income and expense items. Based on your industry code, the IRS computers use formulas to evaluate your return for reasonableness. If your income is out of proportion to your claimed expenses, or if you have deductions not typical for your industry, your return may be flagged for audit.

10 Tips for Keeping an Eye on Finances

1. **Review bank statements.** In today's world of automated banking, downloadable bank transactions and computer reconciling, it's easy to overlook a review of the bank statement for irregularities. More common than fraudulent transactions are mis-read checks (incorrect amount) and unexpected charges (bank computer mis-coding).
2. **The Treasurer should review all bank statements and financial activity.** The Treasurer has primary responsibility for all financial accounts of the organization. However, it is sometimes more efficient to delegate a particular account to a second person (for an event or specific program). The "checkbook" might be in the hands of another, but the bank statements and responsibility still rest with the Treasurer, and all paperwork should be submitted to the Treasurer in a timely manner.
3. **Appoint a second person to review bank statements.** In addition to your Treasurer, appoint a second person to take a look at the bank statements each month.
4. **Review bank statements monthly.** Even if you have minimal activity in a month, it is important to review and reconcile your bank statements monthly in order to catch problems and resolve them quickly.
5. **Have on-line access to your account.** The Treasurer and one other officer should have on-line access to the nonprofit bank account. This will allow you to look for specific transactions, find transaction codes, and see check images. This also extends your "viewing window" both back in time (for old transactions) and today (for transactions that have cleared the bank but have not been sent to you in a bank statement).
6. **Act on mistakes promptly.** You have 60 days from the date of the bank statement to notify the bank about an error - regardless of whose error (bank error, your error, payee error). Notify the bank as soon as possible and request an investigation.
7. **Notify the bank of theft or fraud immediately.** Banks usually have an 800-number that you can use to notify the bank of a lost or stolen debit card, account theft, or other financial issues that might require immediate action. Don't assume that if an incident occurs over the weekend that you have to wait until Monday morning to take action (i.e. freeze accounts, if necessary).
8. **Request that check images be included on bank statements.** Banks are no longer required to return canceled checks, and might not automatically include check images on the bank statements. Make sure your bank statements include images, so you can verify check payees, number of signatures, and who signed the checks.
9. **Do not assume the bank will catch errors or fraudulent checks/transactions.** Most of banking is automated, and banks are no longer responsible for verification of signatures (either correct signature or correct number of signatures). Banks are not responsible for catching and declining out-of-date checks (over 90 days). It is up to you to follow up on errors or fraudulent use of the banking system.
10. **Get to know your banker.** The more your bank knows about your organization, and the more you know your banking professional, the better your bank can help you - both to plan for the best management of your financial resources and to help you in times of financial crises.

Nonprofit Financial Control Policy

The Board desires to set a tone of accountability for managing finances. This policy establishes controls for handling receipts and disbursements, including notation of what transactions require Board approval.

1. Check-Signing Authority. The board chair, treasurer, chief executive, and one senior staff member other than the director of finance, as designated by the chief executive, are authorized to sign checks.
 - a. One Signature Authorized. Checks up to \$250 require one signature.
 - b. Two Signatures Required. Checks over \$250 require the signature of two of the following: the board chair, treasurer, chief executive, or other senior staff member as designated above.
 - c. Board Approval Required. Board Pre-approval for expenses in excess of \$1000 is required.
 - d. Self-signing Checks Prohibited. No one may sign a check payable to oneself, either as a sole or a secondary signature.
2. Accounting and Cash Management Security.
 - a. Counting Cash. For all fund raising activity or receipts of cash from events, two people will count the cash, together.
 - b. Deposits. All cash and checks will be processed immediately; if deposits cannot be made in a timely manner, checks and cash will be locked in a secure location.
 - c. Computer Controls. Computers will be password-protected and kept in a secure location. Laptops will be stored in a secure location when not in use.
 - d. Reconciling Accounts. All accounts will be reconciled monthly.
3. Cash Disbursements. Cash Disbursements are discouraged; however, an authorized check signer will make disbursements only upon review and approval of the transaction, including review of proper supporting documentation, such as a purchase order and evidence of the receipts of the goods and services.
4. Collection of Funds and Deposits. Ideally, the person that writes checks does not make deposits. For all deposits, careful record funds must be made, including fund account deposited to, purpose of deposit, donor (or payor), and amount. Copies of all checks are encouraged. If possible, deposits should be verified and initialed by another staff or Board member.
5. Board and Staff Fiduciary Duty. It is the duty of any Board and Staff member who has authority to sign check to verify that there are sufficient funds available for payment of the checks before affixing his or her signature.
6. Board Approval Required for all Credit and Borrowing Transactions. Board approval must be obtained for all applications of credit and loans. At least two signatures, at least one of which must be a Board Member, are required to obligation Acme for any loan or extension of credit.
7. Credit Cards and ACH Payments prohibited. Except for payroll and as otherwise specifically approved by the Board, use of company credit cards or ACH payment of expenses is prohibited.
8. Annual Audit or Review. The Board will conduct an annual audit or review of the financial accounts. If a third-party audit is not feasible, at least one Board Member, other than the Treasurer, will review all income and expenses, bank statements, and account balances for the year. A report will be made to the Board of any findings

Document Destruction Guidelines

The Sarbanes-Oxley Act addresses the destruction of business records and documents and turns intentional document destruction into a process that must be carefully monitored.

Nonprofit organizations should have a written, mandatory document retention and periodic destruction policy. Policies such as this will eliminate accidental or innocent destruction. In addition, it is important for administrative personnel to know the length of time records should be retained to be in compliance.

The following table provides the minimum requirements.

This information is provided as guidance in determining your organization's document retention policy.

Type of Document	Minimum Requirement
Accounts payable ledgers and schedules	7 years
Audit reports	Permanently
Bank Reconciliations	2 years
Bank statements	3 years
Checks (for important payments and purchases)	Permanently
Contracts, mortgages, notes and leases (expired)	7 years
Contracts (still in effect)	Permanently
Correspondence (general)	2 years
Correspondence (legal and important matters)	Permanently
Correspondence (with customers and vendors)	2 years
Deeds, mortgages, and bills of sale	Permanently
Depreciation Schedules	Permanently
Duplicate deposit slips	2 years
Employment applications	3 years
Expense Analyses/expense distribution schedules	7 years
Year End Financial Statements	Permanently
Insurance Policies (expired)	3 years
Insurance records, current accident reports, claims, policies, etc.	Permanently
Internal audit reports	3 years
Inventories of products, materials, and supplies	7 years
Invoices (to customers, from vendors)	7 years
Minute books, bylaws and charter	Permanently
Patents and related Papers	Permanently
Payroll records and summaries	7 years
Personnel files (terminated employees)	7 years
Retirement and pension records	Permanently
Tax returns and worksheets	Permanently
Timesheets	7 years
Trademark registrations and copyrights	Permanently
Withholding tax statements	7 years

©2004 National Council of Nonprofit Associations, www.ncna.org

May be duplicated for non-commercial use, with attribution, by charitable organizations.

The National Council of Nonprofit Associations (NCNA) is the network of state and regional nonprofit associations serving over 22,000 members in 46 states and the District of Columbia. NCNA links local organizations to a national audience through state associations and helps small and mid-sized nonprofits: manage and lead more effectively; collaborate and exchange solutions; save money through group buying opportunities; engage in critical policy issues affecting the sector; and achieve greater impact in their communities.

Save-The-World Nonprofit Conflict of Interest Policy

Section 1. General. The Board and Staff of STW NonProfit shall administer the affairs of STW NonProfit honestly and economically and exercise their best care, skill, and judgment for the benefit of the STW NonProfit. The Officers shall exercise the utmost good faith in all transactions relating to their duties for the STW NonProfit. In their dealings with and on behalf of STW NonProfit, they are held to a strict rule of honest and fair dealings. They shall not use their position, or knowledge gained therefrom, so that a conflict might arise between the STW NonProfit interest and that of the individual or an organization affiliated with the individual.

Section 2. Disclosure of Potential Conflict. Any officer, Director or Staff member of STW NonProfit shall have a duty to disclose any potential conflict of interest by virtue of business or charitable affiliation.

Section 3. Conflict of Interest Defined. A conflict of interest, or potential conflict of interest, or appearance of conflict of interest, occurs when an officer, Director, or Staff member of STW NonProfit is in a position to exert influence, in dealings with or on behalf of STW NonProfit, which would give preference to any other business or charitable organization with whom the officer, Director, or Staff member is affiliated, by virtue of employment with, membership in, ownership of, appointment to or election to said business or charitable organization.

Section 3. Waiver of Conflict. Whenever a conflict of interest arises, or the appearance of a conflict of interest, such director or officer with the conflict who is present at the meeting of the Board of Directors or of a committee of the Board, shall disclose in good faith the material facts as to such interest, or financial interest, or appearance of conflict of interest, and any action of the Corporation to approve activity in which a conflict of interest, or appearance of conflict of interest, exists, shall be approved by a majority of the disinterested directors.

Conflict of Interest – Board Member Affirmation and Disclosure Statement

My answers to this disclosure form are correctly stated to the best of my knowledge and belief. Should a possible conflict of interest arise in my responsibilities to the Corporation, I recognize that I have the obligation to notify, based on my position, the appropriate designated individual (President of the Board and/or the Board of Trustees), and to abstain from any participation in the matter unless and until the Corporation can determine whether a conflict exists and how that conflict shall be resolved. If any relevant changes occur in my affiliations, duties, or financial circumstances, I recognize that I have a continuing obligation to file an amended “Conflict of Interest Disclosure Form” with the appropriate designated office.

I understand that the information on this form is solely for use by the Corporation and is considered confidential information. Release of this information within the Corporation will be on a need-to-know basis only. Release to external parties will be only when required by law and/or federal regulations.

Signature

Date

Please complete the following questions, and submit this form to the Board President.

1. Are you or a member of your immediate family an officer, director, trustee, partner (general or limited), employee or regularly retained consultant of any company, firm or organization that presently has business dealings with the Corporation or which might reasonably be expected to have business dealings with the Corporation in the coming year?

_____Yes _____No

If yes, please list the name of the company, firm or organization, the position held, and the nature of the business which is currently being conducted with the Corporation or which may reasonably be expected to be conducted with the Corporation in the coming year:

2. Do you or does any member of your immediate family have a financial interest, direct or indirect, in a company, firm or organization which currently has business dealings with the Corporation or which may reasonably be expected to have such business dealings with the Corporation in the coming year?

_____Yes _____No

If yes, please list the name of the company, firm or organization, the nature of the interest and the name of the person holding the interest, and the nature of the business which is currently being conducted with the University or which may reasonably be expected to be conducted with the Corporation in the coming year:

3. Do you or does any member of your immediate family have a financial or personal interest in an entity in which the Corporation has a financial or other vested interest?

_____Yes _____No

If yes, please provide details below:

4. Have you or an immediate family member accepted gifts, gratuities, lodging, dining, or entertainment that might reasonably appear to influence your judgment or actions concerning the business of the Corporation?

_____Yes _____No

If yes, please provide details below:

5. Do you have any other interest or role in a firm or organization, where that interest or relationship might reasonably be expected to create an impression or suspicion among the public having knowledge of your acts that you engaged in conduct in violation of your trust as a trustee, officer, faculty or staff member?

_____Yes _____No

If yes, please provide details below:

Please add additional pages as needed.

If any material changes to the responses provided on the annual disclosure form occur before the next form is due, the trustee, officer or employee is required to update the information on this form in writing, and submit the update to the Board President.

Acme Nonprofit Risk Management Policy

Acme Nonprofit is committed to protecting its human, financial, tangible, real estate, and goodwill assets and resources through the practice of effective risk management.

Acme's board and management are dedicated to safeguarding the safety and dignity of its paid and volunteer staff, its clients, and anyone who has contact with the organization. To this end, the board will ensure that the organization has a risk management plan for the organization that is reviewed and updated on an annual basis.

1. Policy Overview. Financial resources of Acme are the responsibility of the board of directors. The board will:
 - a. Have a clear plan for acquisition of financial resources to pay for the programs and services provided by Acme
 - b. Provide guidelines for management and allocation of financial resources which will produce optimum benefit for those we serve.
 - c. Monitor and evaluate the financial plans and guidelines of Acme to ensure the financial integrity of Acme

2. Budget. An annual operating budget will be prepared by the executive director and presented to the board for approval at least 60 days prior to the beginning of the next fiscal year. The budget will reflect the cost of carrying out the programs and services of Acme for the next fiscal year. This budget will also reflect the anticipated revenues of Acme.

3. Budget Review and Implementation. The budget will be viewed by the board as the financial plan for Acme, and approval of the budget by the board will be authority for the executive director to manage Acme's finances according to the plan without seeking further approval of the board. However, the executive will keep the board well informed of the ongoing status of the financial plan, and will not make expenditures outside of the budget plan without seeking board approval to amend the budget. Amendments to the budget will be presented to the board for approval for any of the following reasons:
 - a. Acme enters into compacts or contracts that were not included in the approved budget.
 - b. Management proposes a major expenditure that was not included in the approved budget.
 - c. Significant unanticipated revenues are received or cost overruns occur

4. Capital Reserves. A working capital reserve sufficient to keep Acme operating for at least a 60-day period will be maintained at all times.

5. Accounting Systems. The accounting system used by Acme will utilize generally accepted accounting practices (GAAP) that are required and/or recommended by regulatory or lending agencies and the Acme auditor.

10 Ways to Catch Fraud (and Mistakes) from Outside the Nonprofit

Fraud and error can occur both within and without an organization. Your employees and board may be completely trustworthy, but fall prey to a number of scams that are now more frequently targeting nonprofit because of the general trusting nature that is part of nonprofit culture. Here are some tips to help you catch outside fraud (or mistakes) before it affects your bottom line:

1. **Verify all packing slips and receipts.** When orders are delivered, (or at the check-out counter, if purchases are made in-store) double-check packing lists and receipts against orders to be sure that you have received all you were billed for, and haven't been double-billed for an order.

2. **Verify all invoices**
 - a. **(part 1 - error)**. Before writing the check, be sure that you haven't already paid a bill. Because of the economy and increased need for immediate cash flow, many vendors are accelerating their payment cycle, and you might get a "reminder invoice" close in time to receipt of the original invoice.

 - b. **(part 2 - fraud)**. Make sure you have actually received the product for which you have an invoice. There have been recurrences of an old fraud scheme to bill a customer for a product that was never ordered and never received, on the theory that the accounting department will routinely pay any bill that looks "legitimate."

3. **Never place orders with cold-callers.** No matter how great of a "deal" a cold-call sales person might have, NEVER place an order with an unfamiliar vendor that calls you. This, too, is an older scam that has been resurrected as a result of the poor economy.

4. **Use Bids for Larger Purchases and Service Contracts.** Get a second (or third) quote or bid for larger purchases, such as HVAC improvements and repairs, computer and network purchases and installation work, and office improvements. Check references for new contractors, such as outsourced payroll and benefits services, building repair and services, HVAC contractors and custodial services.

5. **Watch Outsourced Services.** Monitor third-party payroll and accounting services to be sure that the work is accurate and timely, including required government reports. If you use a third-party fund-raising service, be especially vigilant of over-reporting and hidden fees.

6. **Use Conservative and Rated Investment Services.** For nonprofits lucky enough to have endowment funds, investments, and reserves, place these funds with reputable and rated investment firms. Ask a board member familiar with banking and investment practices to review the investment statements to be sure that the investments are appropriate for a nonprofit (nonprofits are held to a “prudent investor” standard of care, and prohibited from making risky or speculative investments).

7. **Closely monitor cash events.** Have at least two vetted volunteers monitor cash receipts at events where cash plays a large part of the revenue (gate receipts, cash sales or products at an event, silent auction payments). Insist on taking your time to calculate amounts due and in counting money. It is very easy to scam cash when there is a crowd of people competing for the person “running the till” at a cash-intensive event.

8. **Pursue bad checks.** It is tempting to “let go” bad checks because of the hassle involved - especially when a small amount is involved. Knowingly writing bad checks is a criminal offense, and can be costly to the nonprofit in bank fees. Have a system and policy to pursue repayment of bad checks, and (if necessary) keep a list of and enforce “cash only” customers.

9. **Verify Credentials.** Verify credentials of any professional services you partner with or hire. Many times, a quick “Google” search will confirm (or not) credentials claimed by a new acquaintance/potential project partner. Watch for suspicious “blanks” in someone’s history or credentials, or credentials that seem “too good to be true.” Ask for and check references.

10. **Secure the Premises.** Have a practice of locking all doors when the nonprofit business is closed and organize your office space for secure and monitored access during the day. Is the door visible from the office so someone can monitor public traffic? Are valuables (cash, computers, supplies) secured from public access during business hours? Is someone ALWAYS in the office during business hours or when the office is accessible to the public?
 - a. Apply a philosophy of security to any public event sponsored by the Nonprofit to extend physical security practices to event sites.
 - b. Don’t forget to secure computers from outside invasion. Be sure the software monitoring, virus and spyware is up-to-date and activated. Safeguard and use passwords for computer access, and backup regularly.

15 Ways to Minimize Employee Fraud

Financial Controls to Minimize Employee Fraud

1. Perform a background check on all new hires. The Board should have a policy of performing a criminal background check (called “Limited Criminal History Check”) on all new hires. Require the candidate to provide references and CALL the references (and listen “between the lines” to what is said) Don’t get pressured by the need to fill a vacancy or by the candidate’s self-disclosed “other options.” Check before you hire.
 - a. Are Credit-checks legal? Do they work? A new trend in employee background checks is to also conduct a credit check. This can verify whether a candidate pays bills on time, and can be helpful in verifying previous addresses and employment. This information can provide clues about a candidate’s level of responsibility. You must obtain the candidate’s permission before on a separate consent form prior to running the check.
 - b. If you decide to NOT hire a candidate based upon credit check results, you MUST inform the candidate of the reason and provide a copy of the adverse credit report, including the contact information for the credit reporting agency that provided the report. You must also keep the results of the credit check confidential (regardless of the results).
2. Require two signatures on checks. Depending on your corporate structure, you can limit the two-signature requirement to checks above a certain threshold (for example, \$250 or \$500), or require two signatures on ALL checks.
3. NEVER pre-sign checks. This is not only a “bad idea,” but compromises the nonprofit’s financial integrity. What would the public say if they knew that you allowed pre-signed checks?
4. Do not allow one person control over all accounting functions. This is also called “separation of duties,” and provides both an actual and psychological barrier to fraud. Examples:
 - a. The person that writes the checks does not sign the checks.
 - b. The person that makes the deposits does not count the cash.
 - c. The person that opens the mail does not count the deposits
 - d. Two people count cash receipts (particularly for events that generate a lot of cash)
 - e. The person that reconciles the check book with the bank does not handle the money
 - f. Cross-train employees to cover for vacations and illnesses
5. Consolidate Checking Accounts. Talk to your banker about consolidating checking accounts. Usually, computer programs are very good about segregating project funds, so if you don’t have a need (or supervising agency requirement) for separate bank accounts, consider consolidating the accounts. If you must have more than one account, use the same bank and make sure the banking staff knows you and your organization. This will discourage “phantom accounts,” which can be used by employees for skimming.

6. Eliminate petty cash. These days, there is very little requirement for cash, and petty cash can often be overlooked and easily “skimmed,” since it fosters a more lack accounting.
7. Have an outside auditor review the books. At least annually for most nonprofits, and more often for larger nonprofits or nonprofits that have a significant amount of government money (either tax dollars or grant funds), an outside party should take a look at the books.
8. Use a computer program to enter all financial activity. Even very small nonprofits can afford some of the “consumer-based” accounting packages that are both inexpensive and easy to use. Computer data that is regularly reconciled with company documents and bank statements can quickly show discrepancies and omissions that may lead to discovery of fraud.
9. Use Budgets. Consistent use of budgets and comparison of cash flow to budget expectations can reveal unexpected expenses or discrepancies in expected income
10. Look for Ways to Improve. Encourage employees to suggest improvements to the financial system.

Corporate and Procedural Controls to Minimize Employee Fraud

11. Watch Employee Hours and Overtime. Verify employee hours, particularly overtime hours, to be sure that there is not “padding.” This is also true for compensatory time (Comp Time) – inflated Comp Time is the same as padding paid hours.
12. Watch Corporate Stock and Inventory, Including Supplies. In today’s economy, employers are recording an increase in theft of office supplies and corporate inventory. Even larger items, such as computers and cameras have been reported stolen by employees. Note if office supplies seem to be depleting more rapidly than expected, or if sales revenue does not match inventory sold.
13. Watch Expense Accounts. Require receipts for all reimbursements (including board reimbursements) and do not allow anyone to approve his or her own expense reports. Verify requests for reimbursement (Does mileage match approved destinations? Were purchases approved? Is there a “cap” for reimbursement of meals?)
14. Verify Credit Card Charges. It can be “too easy” for employees to purchase items using the company credit card. Over the past several years, there have been several stories of executive staff using nonprofit credit cards personal purchases, particularly when the credit card statements are not closely reviewed and receipts matched with charges, and when the executive is the one that processes the credit card statements
15. Routinely Review Bank Statements. Appoint someone outside of the financial routine to review bank statements. Many banks include check images and deposit slip images with the bank statements, which can be a quick way to review and verify checks and catch patterns of improper payments, overpayments and duplicate payments (whether deliberate or mistaken).

BONUS TIP: Set the tone at the top: promote high ethics and create a code of conduct and conflict of interest policies that reflect your culture and encourage ethical behavior at all levels.

Someone Stole The Cashbox!

Personnel Matters in Nonprofit Fraud or Theft

A feeling of dread sets in when nonprofit officials discover fraud or theft in their nonprofit. Nonprofit organizations operate in a difficult financial environment; the added burden and betrayal of fraud, embezzlement or theft can trigger a panicked reaction from the decision makers.

If your nonprofit is the victim of fraud, theft or embezzlement, here is a checklist to help manage the first few days and weeks after the discovery and verification of an unexpected loss of funds due to criminal conduct:

1. **If You Suspect Fraud – Act Immediately to protect the nonprofit**
 - a. **Lock-down assets**
 - i. If Data and Dollars - change passwords, verify access (Who has access to the account, who are authorized signators?)
 - ii. If “Physical” assets - change door locks, verify that security systems have not been compromised, account for all keys/key cards
 - b. **Rotate duties**
 - i. Most nonprofit employees are cross-trained by necessity due to staff needing to cover illness and vacation time for other employees. Immediately rotate normal duties to cut off anyone with “guilty access.”
 - c. **Change Procedures - Increase controls**
 - i. Require two signatures on all checks, put an alert at the bank, survey the bank for all account activity and immediately reconcile all accounts with the bank
 - ii. Add a person to income controls - counting cash, processing checks, opening mail - this would be a good opportunity to train a board member in the nonprofit’s financial procedures
 - d. **Contact your accountant (if you don’t have one - get one)**
 - i. Request immediate supervision and review of accounts to confirm fraud (or theft or embezzlement)
 - ii. Ask for audit of previous activities to confirm fraud and identify source or key vulnerabilities
 - iii. Ask for audit to create a “bright line” between “contaminated” financial information and “clean” financial information
 - iv. Request assistance in “starting over” for accounting procedures to recalibrate income and expense controls
 - e. **Consult your attorney for legal guidance and ramifications of suspected fraud**
2. **If you confirm fraud**
 - a. **Manage Assets.** Work with your accountant to address vulnerabilities and implement new or revised controls to prevent future fraud
 - b. **Confront the perpetrator –**
 - i. **If employee –**
 - (1) Review employee manual (or contract) for procedures for suspected theft and follow termination guidelines
 - (2) If no manual or contract, Executive Committee should determine course of action (immediate termination, suspension, reporting to authorities)
 - (3) Confront employee with proof and consequences. If termination, provide an escort to clean out desk, turn in keys and leave the building.
 - ii. **If Officer or Board Member (or significant other of Officer or Board Member)**
 - (1) Consult your bylaws for involuntary removal of officer or board member and follow guidelines, if necessary.
 - (2) Executive Committee or Board President should meet privately with officer or board member, provide evidence of fraud and request resignation
 - (3) If perpetrator is SO of Officer or Board Member, resignation should be requested for the good of the nonprofit
 - iii. **If Volunteer, donor, or other stakeholder**
 - (1) Confront the perpetrator (at least two representatives)
 - (2) Formally sever ties (escort out of building, ask to not come back, “persona non grata” status)
 - c. **Contact police to report criminal activity**
 - i. Cooperate in investigation, provide information but
 - ii. Protect donor privacy, employee privacy, to the extent not involved with the crime

Public Relations in Time of Crisis Keeping Cool When on the Hot Seat

When crisis looms (or crashes), there is little time to react before a story spins out of control. This guide or checklist can help a nonprofit keep cool and maintain public goodwill while managing a crisis.

1. **When crisis is apparent. STOP AND PLAN.** Sit down with the primary decision-makers to develop a written and confidential response strategy.
2. **A crisis response plan should include:**
 - a. Flow of information (who talks to whom, who should be included in key conversations, who should be included in press release and other public response)
 - b. Crisis response planning team - core group and support/implementation group
 - c. Crisis Response Goals – maintain community support, recover lost cash flow, prosecute criminal behavior, implement plan to prevent future vulnerability
 - d. A script for formal response for Spokesperson to use in interviews and press releases
 - e. Public mantra (what everyone except the Spokesperson says to the public) – Public mantra typically is, “Ms. X is our official spokesperson. You should direct all inquiries and comments to her.”
 - f. Spokesperson marching orders
 - i. What to say
 - ii. Who to talk to
 - iii. When to defer response (when to not talk)
3. **Appoint a Spokesperson.** Qualities of a spokesperson
 - a. Credentials – Executive Director, Board Member, Board Officer, Attorney
 - b. Knowledge – Thorough knowledge of the business practices and programs of the nonprofit, as well as a full understanding of the crisis
 - c. Honesty – Demeanor and presentation are critical. Spokesperson should not demur or dissemble. Even a slight appearance of “hiding something” can damage the Nonprofit’s image
 - d. Ability to handle criticism – The Spokesperson is both the source of information to the public, and the target for negative comments and must be comfortable answering questions and accusations calmly and competently.
4. **Tell the Story**
 - a. Tell it all – don’t hide information just because it’s embarrassing or awkward (but don’t divulge private information)
 - b. Tell it on the record – don’t indulge in private conversations except for a select few (significant stakeholders). Don’t ever talk to the press outside of prepared statements.
 - c. Tell it fast – get YOUR story told before the rumor mill starts
 - d. Tell them what you are doing about it – Have a polished plan to address and overcome the crisis to provide the public with confidence that the nonprofit can survive the crisis
 - e. Get back to work – “Name it, claim it, and move on” – don’t dwell on the crisis - focus on recovery and resuming the nonprofit’s mission.
5. **Discourage prolonged discussion and analysis of the crisis** (by the public and by the nonprofit stakeholders). Once the crisis has been identified, a plan has been developed and implemented, and the public has been suitably informed, discourage continued gossip about the crisis. Instead, gently but firmly redirect the conversation to what the nonprofit is doing now, and the progress and planning that will help the nonprofit recover.

© 2011, Miriam E. Robeson