11 STEPS NONPROFITS CAN TAKE TO MINIMIZE RISK OF THEFT AND FRAUD

Posted on May 3, 2018

Are reports about financial abuses at other nonprofits causing you to reexamine the security of your own organization? In the wake of the recent articles[1,2] on fraud in the nonprofit sector, executives and board members remain busy assuring funders, constituents, and themselves that they too won't end up in the news.

Fraud can occur any time assets are managed without a system of "checks and balances". Many nonprofits operate with minimal overhead, causing overlap of duties and resulting in weakened controls. As organizations grow in size and complexity, more sophisticated systems are required to address the increasing variety and volume of financial transactions.

While it's not feasible to eliminate the possibility of fraud, there are ways to minimize your exposure. Implementing the following procedures will aid in establishing an environment where tight fiscal controls are the norm.

1. Do not delegate e-bill approval or check signing responsibility. Top management is responsible for the finances and should always retain authority for approving payments. Signature stamps are problematic by nature and should be prohibited.
2. Implement electronic safeguards. Make sure you aren't unintentionally giving check signing privileges to those who aren't authorized. Employees with debit cards and electronic access to transfer funds essentially have the same authority as a check signer.

3. Have checks printed directly from your accounting system. Paying bills with system generated checks reduces the risk of alteration. A system reliant on handwritten checks is more vulnerable to document manipulation.
4. When appropriate, let vendors draft routine payments. Allowing certain companies to automatically withdraw their payments is the most efficient way to pay a bill, while also eliminating the chance that your bank account and routing number will fall into the wrong hands.
5. Keep check archives accessible. Make sure your bank returns all original cancelled checks (preferred) or maintains electronic images so that you can easily verify payees. Many banks only provide online access to check images for 90 days.
6. Use two people when processing payments by mail. If your organization receives cash, check or credit card payments, these duties need to be separated and handled by at least two staff members.
7. Always give customers a receipt for point-of-sale (POS) transactions. Since cash registers are most often operated by one person, the receipt serves to verify proper posting of sales. If receipts can't be printed, then be sure the display on the cash register faces the customer so the sale can be verified.
8. Outsource or automate customer payments. A variety of services allow donors and members to make payments by credit card via the web or mobile device. Use a bank lock box if you can't establish separation of duties for payments received by mail. If possible, eliminate all cash and check payments for small transactions.
9. Monitor your revenue. Membership, donor management, and POS systems provide reports to help identify irregularities. Be familiar with key revenue metrics and check them on a regular basis.
10. Know your numbers. Managers who have a firm grasp of their financial results are rarely subject to malfeasance. When management is hands-off, the organization is vulnerable to theft that may go undetected for an extended period.
11. Communicate with staff. Statistically, fraud is most often discovered as the result of a tip. Management must foster a culture where all constituents are encouraged to keep a watchful eye. It is imperative that everyone understands their respective stake in protecting the organizations' assets.

It's important to note that Financial Statement audits are not intended to detect fraud. Their purpose is to validate the accuracy of the financial statements. Although fraud may be discovered during an annual audit, that alone is not an effective measure for prevention.

Relying on outside vendors vigilance is another common error in fraud prevention planning. A misperception exists that banks closely monitor checking accounts. Banks may catch the occasional unauthorized, forged, or missing signature(s), but this is not a reliable method for preventing fraud. Conducting random reviews of bank account activity is the best way to deter felonious activity.

These basic precautions can help protect nonprofits from financial losses and damage to their credibility. Finally, if you are still concerned about the vulnerability of your organization, seek an independent review. Public loss of financial integrity is not the kind of news that any nonprofit should be making.

(1) *Nonprofit Fraud: How Good are Your Internal Controls?*, Strategic Finance, March 2017

(2) *Inside the Hidden World of Theft, Scams, and Phantom Purchases at the Nation's Nonprofits*, Washington Post, October 2013

Author: Tom Joseph, Founder & CEO, Bookminders

*This article was recently featured on the **Maryland Nonprofits** website as a guest blog post.*