Assess Your Organization's Vulnerability to Fraud

It's a people problem, so combat it with governance.

By Laurie De Armond & Gerry Zack

Purchasing schemes, cash skimming, and financial statement fraud are three very different types of fraud that nonprofits must prevent, detect, and insure against. Still, behind each of them – and every variety of deliberate, deceptive act against nonprofits – there's a fundamental and shared dynamic at play.

Fraud isn't just an operational or financial risk. It's inherently a human risk, meaning it often crosscuts numerous functions and departments within a nonprofit organization. Not only that, but the people behind these acts are complex. They're pressured by varying circumstances, motivated by different opportunities, and self-assured by their own unique rationales. Making matters more complicated, fraud isn't always a solo act. In fact, a report by the Association of Certified Fraud Examiners (ACFE) found that 46% of fraud cases involve multiple perpetrators. When fraud occurs, the web of nefarious activity often extends to surprising depths within an organization.

To combat this threat, nonprofits face a critical need to address fraud, starting with more guidance and engagement from leaders and boards to create an anti-fraud environment and oversee a fraud risk management function. One of the most important deterrents of fraud is knowing that the organization's leaders have no tolerance for it, will act accordingly to detect it, and will take appropriate action if they find it. Begin by focusing on these four steps:

1. Find a Catalyst

You need a high-ranking sponsor to get fraud risk management off the ground. This leader's first order of business should be deciding whether the organization's fraud risk management will be integrated into the existing risk management function (which typically focuses on strategic, operational, reporting, and compliance risks) – or whether it will be separate. Either way, the goal is the same: Embed a risk management element into the daily activities of all your personnel.

2. Create Responsibilities & Structures

With your management process in place, establish a governance structure for it, including designated oversight responsibilities at the board level, such as an audit committee. Keep in mind, this framework and the tools your organization uses should be scaled to fit both your size and your available resources. It's impossible to completely "fraud-proof" any organization, so understand the weak points in your infrastructure and organization, and then work backwards to execute your anti-fraud processes. Also, while fraud prevention is ideal, many nonprofits have to weigh the costs and practicality of preventive processes versus detective measures.

3. Engage & Educate

Especially when faced with resource constraints, nonprofits should engage all their staff in an ongoing system of fraud deterrence. Above all, provide your employees with workshops and trainings in which you educate them on why people perpetrate fraud, which red flags to watch for, and what resources – such as whistleblower policies, reporting systems, and hotlines – are available to them. Awareness throughout your organization can be the single most effective fraud deterrent and vehicle for detection, but it has to start from the top.

4. Craft Dynamic Risk Assessments

People are dynamic, so your risk assessments must keep pace. With roles and responsibilities identified, use your team to pinpoint which inherent risks exist. Then prioritize these risky situations based on their impact, likelihood, and the speed at which they're apt to occur. Finally, use those priority rankings to map the best preventive and detective controls.

Laurie De Armond, CPA (ldarmiond@bdo.com), is a partner with BDO, a worldwide professional services network of public accounting firms. Gerry Zack, CPA (gzack@bdo.com) is the litigation managing director in BDO's global forensics practice. They write for the Nonprofit Standard blog (Nonprofitblog.bdo.com), from which this article is adapted.

TO SEPARATE DUTIES, THINK LIKE A THIEF

"We don't have enough people to properly segregate duties" is something we hear from many smaller organizations, and even some large ones. Proper separation of duties can certainly be a challenge. One way to simplify it is by thinking like a thief. In other words, consider that in order for crooks to perpetrate fraud, they need to be able to commit and conceal their crimes. If you can segregate the duties necessary to conceal the fraud from the duties necessary to commit the fraud, odds are that the person won't even attempt the scheme.

Sometimes this means simply segregating a single step from the others. For example, many disbursement schemes in which perpetrators write checks to themselves or to personal vendors would easily be detected by having a separate person (often a board member in the case of a small organization) review the canceled checks. Likewise, if you arrange to view cleared checks on your bank's website or receive bank statements directly from the bank, you create an obstacle for a potential fraudster to overcome. What you've done is to segregate the critical concealment step necessary to commit the fraud.

Don't Risk Your Organization's Future

For more on good fraud control, see these articles at NonprofitWorld.org:

Protecting your Organization against Financial Misuse (Vol. 17, No. 4)

Risk Management: How to Protect Your Assets (Vol. 26, No. 1)

Can Your Organization Afford to Lose $100,000? Safeguards Every Nonprofit Needs to Implement (Vol. 30, No. 3)

Wire Transfer Fraud: It Could Happen to You (Vol. 35, No. 3)

RESTRICTED DONATIONS LIMIT FRAUD

A study of IRS records by researchers at William & Mary, Rutgers University, and University of California at Davis, found that nonprofit recipients of restricted donations, such as grants, were 20% less likely to fall victim to fraud than those who received unrestricted donations.

ANTI-FRAUD CHECKLIST

To assess your organization's anti-fraud practices, ask the following questions:

Does your organization have a clearly stated code of conduct that explicitly prohibits fraud and other unethical behavior?

Do managers emphasize the importance of reporting suspected acts of fraud and other ethical breaches?

Do senior managers set an example for all staff by consistently abiding by the organization's code of conduct?

Does the organization have a robust and readily available hotline or reporting system for employees to communicate suspected fraud?

Are there formal procedures for following up on and investigating allegations of fraud, noncompliance, and other ethics breaches?

Does the organization provide fraud awareness training (online or live) that all employees are required to participate in periodically (preferably annually)?

Are employees provided with a confidential way (for example, an employee assistance program) to discuss issues they're facing, such as work-related or personal pressures)?

Does the organization perform periodic fraud and compliance risk assessments?

Is the board of directors or a committee of the board formally charged with oversight of management's fraud risk management activities?

Does the board (or audit committee) receive periodic updates regarding the nature of communications received by the hotline/reporting system and how these communications were resolved/investigated?

Does the board (or audit committee) have formal authority to investigate allegations of fraud, including the ability to bring in outside investigators if deemed necessary?

Does the board (or audit committee) hold discussions with the external auditors regarding the potential for management to override internal controls and what the auditors do in response to this risk?

When violations of the code of conduct are identified, is disciplinary action consistently enforced?

Are fraud and compliance risks included as part of the board's discussions of new programs or other significant strategic changes under consideration?