DECEMBER 2016
www.bdo.ca/not-for-profit

NON-PROFIT

Is Your Non-Profit Fraud-Proof?

Don't overlook these simple ways to reduce your risk

Non-profits are often great places to work. People align around the mission, enjoy what they do, and share a sense of altruistic purpose that brings them together.

But non-profits are no more immune to fraud than any other organization, although statistics to support this are hard to come by. Incidents often go unreported, for fear of damaging their reputation, and potentially drying up their funding sources.

BDO's auditors have encountered cases of fraud risk within non-profit organizations. Yet a few simple but often overlooked safeguards can help you significantly reduce the risk of fraud in your organization.

Cash handling

Cash is inherently risky. It is hard to control, even harder to track, and is the most liquid asset an organization can have.

To reduce the risk, minimize the amount of cash your organization uses. A company credit card for purchases, instead of petty cash, will give you greater control over spending, as well as a clear record of purchases.

Cash donations are less common now that there are so many ways to accept payments electronically, like Canada Helps and Paypal. Credit card donations, too, have never been easier. A simple device and an app for your smartphone can enable you to accept credit card payments almost anywhere you can get cell service.

If you do accept cash donations, make sure you have controls in place to keep track of it. For instance, if you're selling raffle tickets, document the number of tickets in every sale. That way you'll be able to reconcile the money handed in with the tickets handed out, and ensure they balance.

Credit cards

The risk here is that purchases or expenses can be made that are personal or unrelated to your organization's business.

Make sure there's proper documentation, like slips and receipts, for every purchase made. That's the first step.

The second step is to regularly review expenditures, and reconcile the documentation. The purpose of the purchases should be understood and justified.

In general, expenses should always be approved by a person "one level up"—that is, someone who does not report to the person submitting the expenses, and who will not be influenced by them.

Management should also review access to company cards—who needs to have one, and who doesn't. If someone only makes occasional purchases for the organization, it may be better for them to use their personal credit card and submit a claim for reimbursement.

Expense reports

Here again the risk is that the organization will be charged for unnecessary or fraudulent purchases. As with credit cards, this can be easily mitigated in the following ways:

If required travel often follows the same route (such as between offices), institute a standard per-trip payment. Always ask for supporting information or documents, such as a screen shot of an online map.

As with credit cards, consider what was purchased too, and whether it was really necessary.

Establish a "one level up" rule for approvals, and hold everyone accountable. For example, Board members should approve CEO expense reports.

Consider creating standard forms for expense reports, with areas for explanation. Be sure to include space for the name of the person approving the report.

Payroll

If one person is in charge of payroll without supervision or approvals—especially if they have complete online access—the risk of abuse is high. They could raise their own pay, or invent a fictitious employee and collect that salary too.

Your organization should ensure that a complete payroll report, summarizing all staff pay, be printed, reviewed and signed by someone "one level up" from the person processing, every payday.

Proper oversight requires documentation and reconciliation. The payroll report should be compared with the bank's direct deposits report, to ensure they balance.

Online transactions

Online expenditures should be treated the same as any other expense. They need to be documented and approved, to prevent unauthorized payments or fraudulent purchases.

As with credit cards, everyone's online access should be reviewed. Some may need access to do their job, but others won't. Set up specific policies governing who can make purchases, what types of purchases, and who approves it.

Find out what reporting is available. Can monthly transaction reports, for instance, be printed and reviewed at any time?

Some banks offer key encryption systems that require authorization before an online transaction goes through. One person sets up the transaction, and another person (one level up) authorizes it.

Careful control and oversight should be in place for setting up authorized vendors online. Bank reconciliations should be conducted and reviewed each month.

Review transfers between bank accounts to make sure the amounts are correct. Consider setting limits on the size of transfers to or from different accounts.

Signing cheques

A second authorized signature should be routinely required on all cheques—especially if the same person is signing the cheque, recording the purchase, and reconciling the bank statement.

Signing authority should be limited to specific amounts, and preferably specific types of purchases.

Do not depend on the bank to catch unauthorized signatures or single-signature cheques. They don't necessarily look at every cheque—which is why you need to. Make sure the bank returns your cheques, either hard copy or images, and verify them during reconciliation.

Conclusion

Your organization's risk of fraud can be dramatically reduced through simple common-sense precautions.

Most non-profit organizations follow a few principles:

- **Documentation:** Keeping complete records of every transaction makes it easier to track receipts and purchases, and helps to prevent fraud.
- **Oversight:** Approvals should always be made by someone "one level up" from the person requesting the approval. This includes the leadership team.
- **Standards:** If everyone knows and follows the same procedures, it's harder to beat the system.

Most employees are honest—but that's no reason not to take precautions. That's why the last person leaving the office always locks the door.

Fraud-proofing your non-profit can reduce your risks—and allow you to focus on the important work of fulfilling your mission.

To learn more, please contact your local BDO office or:

Tim Sothern, FCPA, CPA, HBA
Partner, Regional Non-Profit Industry Leader
519 576 5220
tsothern@bdo.ca

Christina Brox, CPA, CA
Senior Manager
519 576 5220 Ext 5065
cbrox@bdo.ca

Jayme Ford, CPA, CA
Manager
519 576 5220
jford@bdo.ca

About BDO

One of the nation's leading accounting firms, BDO Canada provides assurance, accounting, tax, and advisory services. As a member of the BDO international network, which spans more than 150 countries and 1,400 offices, BDO provides seamless and consistent cross-border services to clients with international needs.

About BDO's Not-For-Profit and Education Practice

BDO's Not-For-Profit and Education Practice team provides a full range of tailored services to help organizations like yours address their changing needs and identify new opportunities. Our strength and depth of expertise with organizations operating at the local, provincial and/or national levels means that our professionals are able to apply practical knowledge and insight to assist you in addressing the various challenges you face. As a member firm of the international BDO network, we also have access to advisors around the globe with over 1,400 offices in more than 150 countries.