Information Technology Controls for Non-Profit Organizations

by Makaela Rae Clapp, CPA, Senior Associate

Posted on March 21, 2024

A common struggle with smaller organizations is building adequate internal controls, particularly over information technology. While a small entity may not have the same resources as a larger organization, it does have the same responsibility to protect crucial customer, employee, and financial data. We can all agree that each year more and more of our work is completed or stored electronically, which means focusing on controls over information technology is increasingly crucial. With a limited staff or budget, it may seem difficult to prevent fraud or unforeseen technological issues from happening. Do not worry – there are still ways to implement solid internal controls over information technology with limited resources!

Why Do We Need Internal Controls?

First, we must acknowledge that trust is not an internal control. Non-profit organizations exist to help their communities and are staffed by dedicated and hardworking individuals who believe in their organization's mission. You may think it's less likely to occur at an organization that provides so much good to their community. However, even if you have worked with someone for many years and you could never imagine them betraying your organization, you must prepare for the unexpected. That is why having solid internal controls is so important.

Another reason to have controls over information technology is to prevent data loss and disruption to operations. You want to feel secure that you can continue helping your community efficiently without any technological problems or possibly being hacked.

Passwords

The most recent guidance on passwords according to NIST (The National Institute of Standards and Technology) states that password length is more important than password complexity. You should also avoid changing your password too often as people tend to make one small change to the same password, a trend that external hackers use to their advantage.

Dual factor authentication is a great way to double up on password security because it requires both a password and confirmation from your device (like a cell phone) to log in. This can reduce the risk that your account could be compromised by an external party.

Backup Procedures & Disaster Recovery

There is an earlier full-length article from HeinfeldMeech (available here) discussing the importance of properly backing up your files as well as having a dedicated Disaster Recovery Plan for your organization. To summarize, try to utilize multiple forms of backup methods, including at least one remote method, to ensure that no matter what happens you will be able to recover your data. If you cannot remember the last time you backed up your data, then it might be time to consider implementing some new backup controls. If possible, try to automatically back up your data weekly at a minimum or daily.

Have a formal and tested Disaster Recovery Plan in place so that in the event of an unforeseen disaster, such as a power outage, natural disaster, or cyberattack, you can efficiently resume operations as normal. The costs for an organization start to add up if you lose your data and are not able to retrieve it, so it is more cost effective to plan in advance.

Antivirus

It is crucial to have up-to-date antivirus software installed on all devices to prevent viruses and external parties from gaining access to your computer. However, it is important to also practice caution when clicking on links or images in emails or on websites, particularly from emails outside of your organization or websites you do not frequently access. Consider having an annual information security training for your employees so they can learn the most common mistakes and learn what to avoid.

Application Access

Regardless of which accounting software (or even software for other departments) you use, you should make every attempt to limit the amount of access that each employee has to different modules and functions within the application. Every employee should only have access to the functions necessary for their job duties.

This is often very difficult if your organization is especially small, so if you cannot limit application access in a manner that would still leave day-to-day operations efficient, then you should implement compensating controls. This usually involves upper management reviewing

journal entries and reports that are created by other staff. Reviewing financials regularly is also crucial to spot anything out of the ordinary.

You should also ensure that employees who no longer work for the organization have their access revoked as quickly as possible. Do not utilize shared accounts unless necessary so that each account can be audited effectively.

This article certainly does not review everything related to information technology, but summarizes some of the first steps that you can take to help protect your organization. We can never fully eliminate the risk, but we can reduce the risk of IT mishaps from taking basic precautions. Remember that an ounce of prevention is worth a pound of cure!