AICPA® Not-for-Profit Section

IT Controls for Not-for-Profit Entities

Information security is a significant business issue that is only becoming more important as technologies advance and not-for-profits (NFPs) become more sophisticated in using them. Information security threats may be external, as in the case of data breaches or viruses, or internal, as a result of a failure in the design or implementation of IT systems or misuse of data by employees. To protect your organization, consider implementing the following internal controls:

This list includes common controls that are typically considered as part of an NFP's overall IT risk management strategy. All internal controls should be tailored to the organization's size, complexity, risk profile and objectives.

Entity-level Controls

- Convene an IT Steering Committee to prioritize, review and monitor information technology needs
- Formalize your IT policies and train staff and volunteers on its application
- Identify and ensure compliance with laws and regulations regarding information security and privacy
- Assess the adequacy of insurance policies to cover theft, electronic data loss and interruption of operations
- Maintain an IT infrastructure inventory, including software and hardware used (both onsite and remotely), and don't forget to include handheld and mobile devices
- Adopt an incident response plan and establish a team to respond to any information security incidents
- If relying on third-party service providers, obtain the service auditor's report and ensure all recommended security, availability and privacy controls are in place

Access & Security Controls

- Adopt and enforce an Information Security Policy
- Restrict system access to appropriate personnel (based on a documented business need)
- Require a unique ID for each user and limit the use of shared accounts
- Encrypt Operating System drives as well as fixed data drives and removable devices
- Implement access requirements for each application based on business need
- Require password length, complexity, minimum and maximum password age, number of invalid access attempts allowed, and lockout settings
- Review access logs to monitor access to significant applications, especially those of financial consequence to the organization
- Formalize your procedure for addition, modification and termination of user access
- Physically secure all hardware, and require any terminated/exiting employee to return equipment at point of termination

Network Security Controls

- Assign remote access rights based upon business need
- Implement firewalls, intrusion detection and intrusion prevention systems
- Use content filtering controls to review the content of Internet messages for appropriateness and to detect misuse of network resources
- Implement controls over the updating of Operating System "patches"
- Use a reputable anti-virus, anti-spyware and anti-spam software and routinely install updates as they become available
- Perform vulnerability scans and penetration tests of critical systems
- Physically protect servers housing significant data, for example, by using a key lock, smart card, biometric device, or offsite data center

Backup and Recovery Controls

- Maintain a formalized backup policy and schedule
- Determine Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs)
- Implement a system for maintaining backup data
  - examples: off-site media storage, remote backup servers, SANS
- Perform periodic testing to ensure restorability of backup data

Change Management Controls

- Require approval for all change requests
- Maintain a tracking system for all change requests
- Implement a process for migration to new systems
- Maintain a list of individuals authorized to approve and implement changes

The costs of dealing with loss of data can be high. Should an incident occur, NFPs without a plan may waste valuable time trying to organize a core team and determine how to respond. Most proactive organizations create a cross-functional Information Security Response Team. The purpose of having the dedicated Information Security Response Team is to formalize an Incident Response Plan and quickly put the plan into action if needed. Such a plan typically details specific action items and individuals responsible to promptly address issues such as loss of data, theft or data breach if and when they occur. With the proliferation of cybercrimes in recent years, some organizations hire security professionals to perform an IT risk assessment and assist with the development of preventative, detective and reparative procedures to safeguard their organizations.

For additional information, check out these resources:
AICPA's Cybersecurity Resource Center
COSO Internal Control – Integrated Framework
COSO in the Cyber Age IT Risks and Controls in Current and Emerging Environments