



JOHNSON LAMBERT
CPAs AND CONSULTANTS

IT Control Environment: 5 Common Pitfalls for Small NFPs to Avoid

February
2012

Article By: Andrew Pinnero, CISA, Principal, and Mark
Hornby, CPA, CISA, Manager,

Bill Gates once said, "Information technology and business are becoming inextricably interwoven. I don't think anybody can talk meaningfully about one without talking about the other." In the ever evolving world of information technology (IT), this statement has never been truer; no matter the size of the company. In 2006, SAS 109 – *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, was issued, requiring auditors to obtain a more detailed understanding of the entity and its environment, including the IT environment. As a result of this new standard, we had the opportunity to review the IT environment for a wide range of organizations over the years and were able to identify some common pitfalls that can be easily remediated. This article outlines five of the most common pitfalls that we noticed during our audits, the importance of remediation and provide some guidelines for remediation to help align your organization's IT environment and business goals for the future.

Corporate Governance

In a January 2011 survey by the ISACA¹ (ISACA, 2011), it was noted that 94% of those surveyed felt that IT is “very important or important” to the overall business strategy and vision of their organization. In order to obtain this alignment, a governance structure should be implemented to provide direction and oversight to the entire organization, which includes IT. Some items to take into consideration when forming a structure include:

- Ensure that a representative from the IT sector is actively involved in management discussions, for example IT should be part of an organization’s Enterprise Risk Management discussion.
- Ensure that the organization’s Board of Directors is properly monitoring and providing oversight to the IT Function.
- When defining the IT Strategic Plan, ensure that this plan is properly aligned with the overall Strategic Plan.

Documentation of Policies

An old Chinese proverb said, “Ink is better than the best memory.” No matter the frequency that a task is performed or how well the current employees know their roles, policies should be formally documented and approved by senior management. Lack of formal documentation can lead to procedures not being performed in the absence or termination of the employee currently performing the duties. Moreover, there may be instances in which there is no legal basis for the termination of an employee who did not perform their duties in line with these informal policies. In order to mitigate these risks, we would recommend that management performs some of the following steps:

- Identify policies that need to be formally documented (I.E. Disaster Recovery Plan, Data Retention Policy, IT Security Policy, IT Change Policy, Etc.).
- Assign a person to formally document these policies in line with best business practices.
- Once the policies are documented, the management group should review and if satisfactory, approve the policies and determine how they will be enforced.

Network Security Posture

In a recent Cost of Cyber Crime Study conducted by the Ponemon Institute, cyber attacks are up approximately 56% for the same five month period as compared to 2010 (Ponemon Institute LLC, 2011). The same study revealed that the average cost to resolve a cyber attack is \$416,000, but this cost can be significantly reduced with the implementation of proper controls to detect and contain a cyber attack quickly. During the course of our reviews, we noticed numerous instances in which a firewall is improperly installed, not installed in the correct place on the network or the configurations used are set to default. These vulnerabilities can easily lead to potential cyber attacks. In order to mitigate these risks, we would recommend that management perform some of the following steps:

¹ ISACA, formerly known as the Information Systems Audit and Control Association, is an independent, nonprofit, global association that engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems.

- Periodically review your network topology and identify where network access points are located in relation to the firewall, DMZ², Etc.
- Periodically review and test the configuration of your firewall and other security nodes to ensure they are in line with leading business practices.
- Periodically monitor the audit logs to ensure that potential attacks are being identified and addressed in a timely manner.
- Ensure anti – virus and anti-malware are up to date.
- Ensure employees are in tune with organization guidance and security awareness protocols.

Re-Certification

Most organization have controls in place for adding and removing an employee from their system when they are hired or terminated, but how often do you go back and review an employee's access while they are still employed? During the course of our reviews, we noticed numerous instances in which an employee was transferred between departments, while still maintaining access to systems in line with their old duties, resulting in a lack of segregation of duties. IT is occasionally forced to keep both profiles active because the legacy profile is needed to access data in the old department. This access is then forgotten and could be compromised. Additionally, during the course of our reviews, we encountered instances in which organizations exceeded their allotted user licenses amounts, leading to additional costs or fines to the organization. In order to mitigate these risks, we would recommend that management perform the following steps:

- Perform an annual review of users within the network/application to ensure the employee should still have access to the network/application.
- Perform an annual review of the access rights the employee has within the application to ensure the rights are in line with the employee's current job description.
- Review the license agreements for the applications to ensure the organization has not exceeded the allotted user count.

Segregation of Duties

One of the biggest risks for any organization is the lack of segregation of duties within a user's role. This risk could ultimately lead to employee fraud or management override. Organizations typically design their controls to ensure that there are proper checks and balances in place to deter the risk of fraud. This approach should extend from the business process and across the IT environment. During the course of our reviews, we noticed various instances in which developers had access to production data, users were operating under an "Admin" user account, instead of their individual ID, employees were using default vendor accounts that came with the application, and roles within the system were not in line with the employee's current job description (see above). In order to mitigate these risks, we would recommend that management perform the following steps:

- Remove developers' access and other non-essential IT staff access to production data. If the size of the organization is such that the entire IT department consists of one person and access to production is required, turn on the audit logs and assign a non-IT

² DMZ stands for "demilitarized zone," which is a physical or logical sub-network security layer that acts as a buffer between an organization's external services to a large untrusted network.

Manager/Director to periodically review the audit logs. This ensures that there is a business purpose associated with the manager's access to production data and they are being monitored.

- Due to the size of organizations, sometimes it is necessary to assign the Administration rights to an individual user (Admin). The user selected to be the Admin should perform their daily duties under their individual user name and separately perform their administrative duties under the Admin account. Additionally, the organization should identify a separate user to periodically review the activities of the Admin user account.

Bibliography

ISACA. (2011). *Top Business/Technology Issues; Survey Results 2011*. ISACA.

Ponemon Institute LLC. (2011). *Second Annual Cost of Cyber Crime Study; Benchmark Study of U.S. Companies*. Ponemon Institute LLC.

For further information contact:



Andrew Pinnero
732-383-4361
apinnero@jlco.com



Mark Hornby
703-842-1151
mhornby@jlco.com

Andrew Pinnero, CISA, is a Principal, and Mark Hornby, CPA, CISA, is a Manager at Johnson Lambert & Co. LLP. Johnson Lambert is a CPA and consulting firm dedicated to serving the association and non-profit community, employee benefit plans and insurance entities. For over 25 years, we have believed that unique industries demand a targeted focus. We serve a national and selectively international client base including over 200 separate non-profit entities representing over 125 non-profit groups from our offices in Florida, Georgia, Illinois, New Jersey, North Carolina, South Carolina, Vermont and Virginia. Services include financial statement audits, internal control reviews and tax compliance and consultation. For more information about Johnson Lambert & Co. LLP, visit www.jlco.com.