Town of New Canaan, Connecticut

Independent Auditors' Report on Communication of Internal Control Related Matters Identified in the Audit

June 30, 2014

O'CONNOR DAVIES

PKF

Independent Auditors' Report on Communication of Internal Control Related Matters Identified in the Audit

Town Council,
Town of New Canaan, Connecticut

In planning and performing our audit of the financial statements, we considered the Town's internal control over financial reporting ("internal control") to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Town's internal control. Accordingly, we do not express an opinion on the effectiveness of the Town's internal control.

A *deficiency in internal control* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A *material weakness* is a deficiency, or combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A *significant deficiency* is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. However, material weaknesses may exist that have not been identified.

We noted certain other matters that we reported to management of the Town in the attachment that follows.

This communication is intended solely for the information and use of management, the Town Council, others within the organization, and state and federal grantors and is not intended to be and should not be used by anyone other than these specified parties.

December 23, 2014

O'CONNOR DAVIES, LLP
100 Great Meadow Road, Wethersfield, CT 06109 I Tel: 860.257.1870 I Fax: 860.257.1875 I www.odpkf.com

Town of New Canaan, Connecticut

Observations/Recommendations: Internal Control and/or Operating Efficiency

Tax Collections

Tax Collections represents a significant cycle of transactions. Because of the nature of the activity and the lack of rules and regulations regarding internal controls in the State Statutes, there is large risk that errors and/or irregularities could occur and not be noted in a timely manner. The Town has taken steps to address some of these risks. All internal controls that are added should be documented and all steps performed should be documented. (Reported in 2012, 2013 and 2014)

Recommendation: Because of the inherent risk with any Connecticut tax collections office, we would recommend that the internal controls over this system be specifically reviewed and monitored beyond what is required by State Statute. We would recommend that this include at least:

- Periodic and timely reconciliations of the Grand Rate Book Balance Report (GRBBR) to outside documentation including reconciling:
  - The current year's beginning balances to the prior year's ending balances.
  - The current year's levy to the Assessor's Grand List.
  - The lawful corrections to the Assessor's adjustment reports.
  - The total taxes collected to the revenue posted by the finance department.

- Segregation of duties within the tax collection office so that, whenever possible, the following three areas are kept separate:

  - Authorization of transactions
  - Recordkeeping of transactions
  - Custody of assets

  Where a segregation of duties is not possible, other internal control measures should be implemented.

Management's Response: While there are no deficiencies or issues in the Town's Tax Collector's department the Town recognizes that there are areas that could be adjusted or increased in review/reconciliation to prevent risk as found in other municipalities. The Town will work into its reconciliation process between the Assessors department and the Tax Collector's department some of the recommendations of the audit firm.
Response Completion Target Date: *Discussion with Audit firm – processes and procedures are up to date – need to add this language to the department write up. Only issue outstanding is a difference of opinion on the proper handling of cash taken in. Auditor wants only one person touching the cash from the time a tax payer gives the cash to posting to the taxpayers account to the deposit of the cash – management believes there should be segregation of duties and many eyes on the cash with each employee signing off on the ownership of the cash.*

Town of New Canaan, Connecticut

Observations/Recommendations: Internal Control and/or Operating Efficiency (Continued)

General Government

Receiving Reports: There is no policy in place to document that goods were received. The Town assumes the goods were received when the invoice is received.

Recommendation: The Town should consider having the packing slip or other receiving documentation initialed by the receiving party to note that the goods had been received and were not damaged.

Management's Response: The Town requires all invoices to be reviewed by the departments and signed off on as fully received product and or completed services prior to payment. All original invoices are returned to the Finance office for payment after this review has taken place. A more formal receipt of product and or service will be implemented in the new Financial Software system being implemented.
Response Completion Target Date: *As of July 1, 2015 all product or service received goes through a 3 way match – PO must match the receipt of the product or service in MUNIS and match the Invoice submitted to Finance for payment. Departments now have to receive in their product or service within the financial system, verifying they have received and approve of payment for the product or service.*

Purchase Orders: There is no consistent policy for when purchase orders are required. Purchase orders are prepared for some vendors and not for other vendors, regardless of the amount.

Recommendation: A consistent policy should be in place. The policy should (1) make it clear when a purchase order is required and when it is not, and (2) be useful to management in tracking the budget and approving the commitments.

Management's Response: The Town has an unwritten policy but written procedure in place communicated to all departments and controlled by Finance for purchase orders and will revise this procedure into a policy as the new Finance Software system is implemented. The Town requires that all purchases first be requested via a requisition/PO process prior to purchase in order to maintain control over the charter requested appropriation limit set during the budget process.
Response Completion Target Date: *The Town has enacted a Policy that states all purchases or service will require a PO with the exception of a documented list. This was distributed to and communicated to all departments during the training on the new financial system.*

Education

Reconciliation of Records – The Board of Education's General Fund is a subsidiary ledger to the Town's General Ledger. It is not reliable as being complete and accurate unless it is balanced to the General Ledger in a timely manner. The Board of Education and the Town were not able to accomplish the monthly reconciliation between them given manpower issues (Reported in 2012, 2013 and 2014)

Observations/Recommendations: Internal Control and/or Operating Efficiency (Continued)

Recommendation – We recommend that the Board of Education balance with the Town's General Ledger at least monthly. This should be done timely and before the Board of Education's financial reports are distributed outside the finance office.

Management's Response: The Board of Education and the Town have begun to reconcile the BOE subsidiary ledger to the Town's General Ledger.
Response Completion Target Date: *5/30/2015*

Timing of Purchase Orders – The Board of Education requires purchase orders for all purchases. In our sample we noted a large percent of purchase orders were prepared after the date of the invoice. This could have effects on the proper approval of the order and the tracking of the budget.

Recommendation – We recommend that the Board of Education review the purchase order policy to determine if there is a reason that some purchase orders are recorded after the invoice. Purchase orders should only be used when they are useful to management in tracking the budget and/or approving the commitments. The Board of Education should analyze why purchase orders are being prepared after-the-fact and determine if the policy should be changed.

Management's Response: The Board of Education began emphasizing the use of purchase orders, rather than direct payment options in an effort to shift the purchasing culture as well as reflect the new purchasing procedures. Review of process to allow direct payment of smaller purchases will be reviewed.
Response Completion Target Date: *6/30/2015*

Review of Encumbrances – The Board of Education had several encumbrances outstanding at year end that were not actually for firm commitments. These encumbrances had been booked to assist management during the year with their budget projections, but were not cleared at year end. (Reported in 2012, 2013 and 2014)

Recommendation - The Board of Education should perform a final review of encumbrances at year end to be sure that they are for firm commitments in accordance with the Board of Education's encumbrance policy.

Management's Response: Management agrees with the recommendation. Regular aging of open purchase orders will be performed multiple times prior to end of year closing.
Response Completion Target Date: *6/30/2015*

Access to the Electronic Signature Stamp – The Board of Education's checks can be printed with signatures already affixed if someone has access to the signature file. Four of the members of the finance department (Budget Director, A/P clerk, Accountant, and Director of Finance & Operations) have access to the signature file. This includes individuals that are involved in the authorization and recordkeeping of transactions.

Observations/Recommendations: Internal Control and/or Operating Efficiency (Continued)

Recommendation – The Board of Education should review their internal controls to determine if there is an appropriate segregation of duties or offsetting controls.

Management's Response: The Board of Education will evaluate the location of and access to the electronic signature stamp.
Response Completion Target Date: *5/1/2015*

Other Items

Complete Financial Reporting – Currently, individuals outside the finance office are only given budget vs. actual reports from certain funds to review. They do not get all the funds and they do not get balance sheets. (Reported in 2012, 2013 and 2014)

Recommendation – A schedule should be established for financial reporting so that the oversight boards get complete timely reporting that might include: balance sheets, income statements, budget vs. actual reports (annual or project length, as appropriate), and details of programs for funds such as capital nonrecurring, special programs, special educational grants and student activity funds

Town Management Response: The Town has already put in place a quarterly review of all funds and balance sheet account with the board.
Response Completion Target Date: *Completed*

Capital Asset Reporting – We noted that the Board of Education did not include new capital leases as additions to capital assets. In addition, we noted that the Town did not report depreciation expense in the proprietary funds.

Recommendation – Capital asset reporting and reconciling should be included on the month end closing procedures.

Town Management's Response: The Town is hoping with the implementation of the new Financial Software system (same system that the Board of Education is using) that they will have greater access to the details of the fixed assets on the Board of Education side. The new Financial Software system has a Fixed Asset module capable of monitoring fixed assets on a monthly basis.
Response Completion Target Date: *Fixed Asset review has been added to the month end closing schedule.*

Education Management's Response: The Board of Education will work with the Town to establish a procedure to updated BOE capital asset inventory.
Response Completion Target Date: *7/1/2015*

Observations/Recommendations: Internal Control and/or Operating Efficiency (Continued)

Cash Collateralization - The Town may not be taking advantage of certain collateralization set aside on its behalf by the bank.

The Connecticut General Statutes section 36-330 to 36-338 state that any bank holding government money is required to set aside monies to protect those funds. This can total 10 to 20 percent of the balance of public funds.

Under the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA), the Federal Deposit Insurance Corporation ("FDIC") will not recognize a pledge of collateral unless the pledge satisfies the following requirements:

- The security agreement must be in writing between the Town and the bank. Having this requirement in the State Statutes is not good enough.
- It must be executed contemporaneously with the acquisition of the asset by the depository institution.
- It must be approved by the depository institution's board of directors or loan committee, and that approval must be reflected in the minutes of the board or committee.
- It must be an official record of the depository institution continuously since it was executed.

However, Public Law 103-325 (the Riegle Community Development and Regulatory Improvement Act of 1994), which contained a clause revising the "contemporaneous" requirement, was signed by the President in September 1994. Section 317 of the Act states that an agreement to provide for collateralization of deposits of state or local governments shall not be deemed to be invalid under the "contemporaneous" clause of FIRREA solely because the agreement was not executed contemporaneously with the acquisition of the collateral or with changes in the collateral made in accordance with the agreement. As a result, the second requirement above must no longer be met in order for state and local governments to report their deposits as being collateralized. (Reported in 2012, 2013 and 2014)

Recommendation: We recommend that the Town review this and, if deemed necessary, establish collateralization agreements with the banks.

Managements Response: This is an ongoing struggle with the banks that do not recognize the same cash collateralization requirements as the audit firm. The audit firm has offered to communicate directly with the banks for better implementation of this need.
Response Completion Target Date:

Health Insurance Reserve: We noted that the health insurance reserve is not calculated by an actuary.

Recommendation: We recommend that the Town have an actuary review the health insurance reserve.

Management's Response: The Town will consider having an actuary review the health insurance reserve.

IT Observations and Recommendations – Town

IT General Control Assessment

We assessed the Information Technology "IT" general controls of the Town's systems and applications to ensure that policies, procedures, and operational practices were implemented to help support the Town's financial control objectives. We define IT general controls as the following:

> Policies and procedures that relate to many applications and support the effective functioning of application controls by helping to ensure the continued proper operation of information systems. General controls commonly include controls over data center and network operations; system software acquisition, change, and maintenance; access security; and application system acquisition, development, and maintenance. While ineffective general controls do not by themselves cause misstatements, they may permit application controls to operate improperly and allow misstatements to occur undetected. General IT controls need to be assessed in relation to the effect they have on the applications and data that become part of the financial statements.

IT Operations Policies and Procedures

We interviewed various IT department members to assess departmental procedures and requested documentation in support of those procedures. We noted that the Town does not have a comprehensive set of documented standard operating procedures; however, it was clear that the IT department has and follows a strong set of procedures. The lack of detailed policies and/or procedures increases the risk that management expectations and control considerations are not followed consistently. As a result, there is an increased risk that personnel could make errors while carrying out information technology and systems functions. Due to lack of documentation, there is also an increased risk of operation disruption.

We recommend that the Town develop and implement a complete set of standard IT operating policies and procedures. These policies and procedures should be reviewed at a minimum of once annually to ensure that they remain current and accurate.

Management Response: The Town has a working IT policy and it was shared with the IT Auditor. It is a work in progress which we will continue to update. It is in no means a finished project but will making it a priority.
Response Completion Target Date: *In progress and on going*

Innoprise Workflow Administration Monitoring

We reviewed employee access assignments with in the Innoprise system to identify all employees with access to the financial module and to determine if the privileges granted are commensurate with the assigned responsibilities.

The system is configured with programmatic workflows for the approval of purchase orders. We did not identify any control mechanism implemented to effectively monitor the modification and creation of the workflows. Failure to monitor the defined workflows against an approved baseline can result in the creation of rogue workflows that bypass the required approvals.

We recommend that the Town implement a control activity to effectively monitor the established workflows and ensure that all defined workflows are consisted with Town requirements.

Management Response: All Innoprise workflows are reviewed periodically to ensure that no unauthorized changes have been made. The Budget Director/Comptroller and the CFO are the only users with access to change workflow settings.
Response Completion Target Date: *Completed.*

Recertification of Access Rights

The Town does not perform a periodic recertification of user access rights for all network, applications, and folders. This is critical in ensuring that access assignments are appropriate, relevant, and consistent with the expectations of management.

We noted several AD users and computers that did no need to be certain network security groups. Most of the objects were removed during the audit.

We recommend that the Town annually perform a recertification of access rights for all network, applications, and folders. Evidence of the certification should be stored for reference and audit support.

Management Response: The Users where rectified and we have added the annual recertification to our annual internal audit.
Response Completion Target Date: *Completed and July 1st Annually*

Active Directory

Audit Configurations

In review of the various audit settings for the Active Directory domain, we noted that key security events were not configured to audit failures and/or successes of those events. Because the Town does not audit the failure and/or success of certain events (e.g. failed access attempts), the usefulness of the information provided by this detective control is limited.

To enhance the usefulness of this type of detective control, we recommend that at a minimum, the Town consistently audit the following events for both successes and failures for all workstations and servers:

- Account Logon Events
- System Events
- Privilege Use

Management Response: This was rectified and all settings have been applied.
Response Completion Target Date: *Completed.*

Patch Management

Patches are software or operating system updates issued by a vendor to address security and/or functionality problems. Patch management is the collection of processes to ensure that necessary patches are acquired, tested, distributed for installation, and the status of installation monitored and reported on.

We noted during our review that the Town has a patch management process in place to actively distribute, monitor and report on the distribution and installation of operating system and application security patches; however, in our testing of one of the servers, we identified that the server has not been updated in an extended period of time. We noted that the server will be decommissioned but because it is still in the production environment it should be subject to a patch management process.

We recommend that the Town implement a control to alert the IT employees of any servers that have not been updated in a period of time that exceeds the defined deployment schedule so that patches are consistent across servers.

Management Response: The server that was noted has been patched but will be decommissioned in the very near future. For the future, we will look into a notification mechanism.
Response Completion Target Date: *Completed.*

Business Continuity/Disaster Recovery

We noted during our review that the Town's IT department has developed a comprehensive disaster recovery plan; however, no formal documented plan has been created and approved by management to address key parameters such as the amount of acceptable downtime and data loss and system prioritization in the event of a disaster. As result, procedures performed by the IT department might not be consistent with management expectations.

We recommend the Town conduct the following to ensure the existing disaster recovery plan is in alignment with the Town's needs and objectives:

1. Management should conduct a formal assessment to determine how long they can be without the critical servers and network infrastructure. In addition, management should assess how much data can be safely lost before there is significant financial, operational, and image impact. Management should review their operationally critical systems, and based on their acceptable level of risk, prioritize the systems in the order of recovery time (e.g. systems that need immediate recovery versus systems that can wait).

2. Management should formally document all roles, responsibilities, and procedures necessary to accomplish a transition to the recovery site. Standard disaster recovery documents and plans consist of the following phases: Initiation, Activation, Recovery, and Reconstitution.

3. Management should formally document all testing. A comprehensive testing program that is well documented and acknowledged by upper management and key parties will facilitate in continuously improving by adapting to changes in business conditions and supporting expanded integration testing.

Management Response: Within 30 minutes or less our entire data center would failover to our recovery site and is tested on a monthly basis which produces a log which was shared with the IT Auditor. A policy/ procedure document for this was also share with him.
We will work with the administration to address any other concerns or priorities.
Response Completion Target Date: *Completed*

Antivirus

Antivirus is an application that is used to ensure that malicious software is detected and removed in an automated and timely manner.

Although the Town does maintain a comprehensive antivirus system, we noted that a safeguard does not exist to issue e-mail alerts to the IT department for viruses that are detected and not removed. Immediate notification is essential in facilitating a timely corrective response to a virus that has been detected and not removed. Failure to ensure a

timely corrective response can result in unauthorized access, disclosure, modification, destruction and disruption to the Town's systems and networks.

We recommend that the Town implement a mechanism to immediately alert the IT department if a virus is detected and not removed.

Management Response: Updates and scans are done daily.
We will look into setting up a notification mechanism for any potential risk.
Keep in mind we have many layers of protection in place, such as Smart Web filter, Antivirus client/server, redundant firewall access control lists, and email filtering.
Response Completion Target Date: *July 1, 2015 possibly sooner (budget permitting)*

IT Observations and Recommendations – Board of Education

(See attached separate form for time line of response completion dates.)

IT General Control Assessment

We assessed the Information Technology "IT" general controls of the Organization's systems and applications to ensure that policies, procedures, and operational practices were implemented to help support the Organization's financial control objectives. We define IT general controls as the following:

> Policies and procedures that relate to many applications and support the effective functioning of application controls by helping to ensure the continued proper operation of information systems. General controls commonly include controls over data center and network operations; system software acquisition, change, and maintenance; access security; and application system acquisition, development, and maintenance. While ineffective general controls do not by themselves cause misstatements, they may permit application controls to operate improperly and allow misstatements to occur undetected. General IT controls need to be assessed in relation to the effect they have on the applications and data that become part of the financial statements.

IT Operations Policies and Procedures

We interviewed various IT department members to assess departmental procedures and requested documentation in support of those procedures. We noted that the Organization does not have a comprehensive set of documented standard operating procedures. We noted that the IT Director is in the process of implementing a long term Governance Plan that encompasses IT operational procedure; however, the current lack of detailed policies and/or procedures increases the risk that management expectations and control considerations are not followed consistently. As a result, there is an increased risk that personnel could make errors while carrying out information technology and systems functions. Due to lack of documentation, there is also an increased risk of operation disruption.

We recommend that the Organization develop and implement a complete set of standard IT operating policies and procedures. These policies and procedures should be reviewed at a minimum of once annually to ensure that they remain current and accurate.

Munis Access Assignment

We reviewed employee access assignments with in the Munis system to identify all employees with access to the financial module and to determine if the privileges granted are commensurate with the assigned responsibilities.

In our review, we noted a set of employees with privileges in excess of their assigned responsibilities. For multiple employees, full system administrator access was assigned; as such the employees have unrestricted access to all the financial ledgers and functions in addition to user security management (e.g. adding and modifying employee access). The level of access assigned to these employees results in a less than effective set of controls within the application to segment incompatible roles and responsibilities. As such, there is an increased risk of erroneous or fraudulent activities.

We recommend that the Organization perform a complete analysis of all users and access assignments and ensure that the privileges assigned are commensurate with the responsibilities. In addition, access should be assigned with the intention of separating incompatible functions to facilitate the prevention and detection of erroneous transactions or fraudulent activities.

Recertification of Access Rights

The Organization does not perform a periodic recertification of user access rights for all network, application, and folder access rights. This is critical in ensuring that access assignments are appropriate, relevant, and consistent with the expectations of management. We recommend that the Organization annually perform a recertification of access rights for all network, applications, and folders. Evidence of the certification should be stored for reference and audit support.

Documentation of Changes to IT Resources

Any proposed change to IT resources must be approved, tested and documented. We found no formal process for approving, testing and documenting such changes. Such formal process will ensure that no changes to the systems and IT operating environment are unauthorized, untested and untracked.

We recommend that the Organization implement a formal process to ensure that significant changes to the key information resources are formally approved, tested and documented. This is specifically important for any changes or upgrades to the new financial application to be implemented in the near future.

Active Directory

Active Directory is the directory service used by the Organization to provide authentication, account management and system policy control. Active Directory provides the basis for account and system security for all the users and systems on the network. We reviewed various aspects of Active Directory control and management. We noted the following:

Active Directory Password Controls

We reviewed the design and implementation of the password controls of the Organization to ensure that the controls in operation would reasonably protect against unauthorized access to system and network resources. We observed that the Active Directly password controls implemented by the Organization remain significantly weak and no changes have occurred since the last review in 2012. We again noted the following:

- Passwords have no minimum length requirement. An employee can select a blank password.

- Passwords have no complexity requirements. Complexity ensures that a password has a minimum combination of character types (i.e. upper and lower case letters, numbers, and/or special characters).

- Employees are not required to change their passwords. The effectiveness in a password preventing unauthorized access decreases overtime.

- No control exists to lock an account and prevent additional login attempts after a repeated number of failed login attempts. This would allow an intruder an infinite number of repeated password guessing attempts.

We recommend the following minimum password parameters:

- Passwords are required to be at least 8 characters long.
- Passwords are subject to change every 60-90 days.
- New passwords must be different from the 5 previous passwords.
- Passwords must contain at least three of the four character types.
  - Upper-case alphabet characters (A....Z)
  - Lower-case alphabet characters (a.....z)
  - Numbers (0...9)
  - Non-alphanumeric characters (e.g., !$#@%$)
- Employee accounts are locked out after 10 unsuccessful login attempts (locking an account will prevent additional authorization attempts).
- A locked account as a result of failed login attempts is to remain locked for 30 minutes or until administrator intervention.

Separation of IT Employee Accounts for Administration and Normal Business Activities

We noted during our review that the IT employees do not have separate logon id's for the purpose of normal business use (i.e. e-mail, web browsing, etc.) and administrative functions (i.e. account creation, password reset, server support, etc). The IT employees will log on to their workstations with the privilege set assigned to them as members of one of the Active Directory administrative security groups (Domain Administrators, Enterprise Administrators etc). Because the IT employees use a privileged account to perform non-administrative functions, there is an increased risk that these accounts will be compromised by malware, spyware etc. If an IT employee's workstation is infected with some form of malicious software, the security of the entire network can be compromised.

We still strongly recommend that the IT employees use separate distinct accounts for the purpose of normal business use and administrative functions.

Audit Configurations

In review of the various audit settings for the Active Directory domain, we noted that key security events were not configured to audit failures and/or successes of those events. Because the Organization does not audit the failure and/or success of certain events (e.g. failed access attempts), the usefulness of the information provided by this detective control is limited.

To enhance the usefulness of this type of detective control, we recommend that at a minimum, the Organization consistently audit the following events for both successes and failures for all workstations and servers:

- Account Management
- System Events
- Privilege Use

In addition, we recommend that the default size of the security logs be increased to a size that will capture and preserve a period of transactions deemed necessary by the Organization (e.g. the prior 60 days etc).

Timely Notification of Employee Terminations

We reviewed the employee termination process for both accuracy and timeliness. Failure to ensure the accurate and timely notification of employee terminations can result in the unauthorized access, modification, and/or destruction of system and network resources.
We were informed that contentious employee terminations will result in the immediate notification to the IT department; however, during our testing of the termination process, we identified a series of active accounts for terminated employees. In addition, we noted that devices that are assigned to individuals are assigned by the IT Department. As such, if IT is not notified of the Termination, the assigned asset may not be reclaimed.
We recommend that human resources, in conjunction with the IT department, develop a formal workflow and set of procedures to ensure the timeliness, accuracy and accountability of the termination process. The workflow should be designed to incorporate the termination

of user accounts across all applications and to ensure the collection of all Organization IT assets.

Local Administrator Accounts

Local administrators of a system have full access to modify the configurations of that system. This increased level of access substantially increases the risk of virus infection, unauthorized software installation, and unauthorized local system modification. Employees configured with user only rights, as opposed to administrative rights, do not pose the same security risks and help maintain the integrity, security and availability of the system and its environment.

We were again informed that all employees are local administrators to their machine.
We realize certain applications may require local administrator privileges. In most cases, Vendors will provide instructions on how to ensure the correct operation of their software without requiring the user to run as a local administrator. In addition, third party software exists to facilitate application operation without users being local administrators. We recommend that the Organization, if possible, remove the local administrative rights for all employees.

Automatic Workstation Locking

Automatic workstation locking is a technical control by which the system will require the employee to re-enter their password after a period of inactivity to prevent unauthorized access and usage of the system. A technical control is any control that is enforced by the system.

We noted that the current policy forces workstations to lock after 60 minutes of inactivity; however, the control as designed is less than effective in preventing unauthorized usage of idle and unattended workstations.

We recommend that a control mechanism is implemented to lock the workstations after an idle period of 15 to 30 minutes.

Patch Management

Patches are software or operating system updates issued by a vendor to address security and/or functionality problems. Patch management is the collection of processes to ensure that necessary patches are acquired, tested, distributed for installation, and the status of installation monitored and reported on.

We noted during our review that the Organization does not have an effective patch management process in place to actively distribute, monitor and report on the distribution and installation of operating system and application security patches. Without a reliable patch management process the stability, availability, and security of the environment that supports the key financial and operational control objectives are at risk.

We recommend that the Organization implement and deploy an application that will allow it to effectively distribute, monitor and report on the distribution of application and operating system security patches.

Backup Management

We reviewed the backup procedures of the Organization to ensure that that the backups have relevant data selected for inclusion, are monitored for success or failure, and securely stored should restoration be needed.

During our review of the backup management process, we noted the following:

- No formal procedure exists to validate the integrity of the backed up data through the implementation of scheduled data restoration testing.

We recommend that semi-annually, data recovery procedures should be tested to verify data recoverability. Evidence of the testing should be stored for reference and audit support.

Business Continuity/Disaster Recovery

We noted during our review that the Organization has no defined and documented IT disaster recovery/business continuity plan and/or policy. Without a formal plan that will dictate and clarify the roles, responsibilities, and steps necessary for the Organization to perform in the event of a disaster, the Organization is at risk for failure to successfully and quickly recover.

We recommend that the Organization perform the following to mitigate the risk of failure to recover:

1. Management should conduct a formal assessment to determine how long they can be without their functioning servers. In addition, management should assess how much data can be safely lost before there is significant financial, operational, and image impact. Management should review their operationally critical systems, and based on their acceptable level of risk, prioritize the systems in the order of recovery time (systems that need immediate recovery verses systems that can wait).

2. Management should formally document all roles, responsibilities, and procedures necessary to accomplish the transition to the recovery site. Standard disaster recovery documents and plans consist of the following phases: Initiation, Activation, Recovery, and Reconstitution.

3. Management should periodically test this plan for functionality as well as practicality.

Anti-virus

Anti-virus is an application that is used to ensure that malicious software is detected and removed in an automated and timely manner. Anti-virus is the cornerstone of any information security program.

Although the Organization does maintain a central antivirus system, we identified the following:

- A set of workstations that did not have up-to-date anti-virus signatures.
- Two servers that did not have an anti-virus application installed.

We recommend that the Organization implement a series of controls to ensure that anti-virus is installed, active and up-to-date on all workstations and servers at all times.

Network Device Configuration and Management

We assessed the network infrastructure to identify any weaknesses in management and configuration. We sampled a set of devices in the network (i.e. firewalls, switches, etc.) at various locations and the central data center. We identified multiple weaknesses in the configuration and management of these devices. We noted the following:

Firewall Traffic Restrictions

The firewall is the network device that functions as the primary barrier for the internal network against the internet. Without a proper level of restrictiveness in the type of communications that can or cannot cross the firewall, the Organization is at risk for potential covert channels of communication through the firewalls. These channels of communication can be used to facilitate the malicious objectives of malware, spyware, or any other harmful application. These objectives can include, but are not limited to, unauthorized access, unauthorized information leakage and unauthorized resource usage.

We noted in our review of the firewall configurations that the firewall is not configured to restrict outbound and inbound communications to only authorized protocols and services.

We recommend that the Organization increase their level of restrictiveness on its firewall and only allow the communications necessary for the Organization to maintain operations. This will safe guard In addition, access rules on the firewall should be reviewed at annually to ensure that the rules are accurate and relevant for the Organization’s operations.