Town of New Canaan, Connecticut

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

June 30, 2012

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 governmental activities, the business-type activities, the discretely presented component unit, trust funds, each major fund, and the aggregate remaining fund information of the Town of New Canaan, Connecticut ("Town") as of and for the year ended June 30, 2012, in accordance with auditing standards generally accepted in the United States of America, we considered the Town's internal control over financial reporting as a basis for designing our auditing procedures for the purpose of expressing our opinion 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.

Our consideration of internal control was for the limited purpose of conducting the Town's audit and would not necessarily identify all deficiencies in internal control that might be significant deficiencies or material weaknesses and therefore, there can be no assurance that all deficiencies, significant deficiencies, or material weaknesses have been identified. However, as discussed below, we identified certain deficiencies in internal control that we consider to be significant deficiencies, deficiencies that we consider to be control deficiencies and other observations and recommendations for strengthening internal control and/or operating efficiency.

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 significant deficiency is a deficiency, or 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. 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.

The exhibits set forth below and appended to this letter, include our required communications and various matters involving internal control that we identified during our audit.

- Addendum A - Deficiency in internal control that we consider to be a material weakness and significant noncompliance

- Addendum B - Other observations and recommendations for strengthening internal control and/or operating efficiency

- Addendum C – Information Technology observations and recommendations at the general government

- Addendum D – Information Technology observations and recommendations at the Board of Education.

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.

O'Connor Davies, LLP

Wethersfield, Connecticut
April 11, 2013

Town of New Canaan, Connecticut

Addendum A

Material Weakness and Significant Noncompliance

Summary of the Finding:

MW-2012-01 – Timely and Accurate Financial Reporting

Criteria – Financial reporting should be timely and accurate.

Condition – The Town did not have timely and accurate financial reporting for the fiscal year.

Effect – Management did not have adequate financial reporting to make decisions and comply with budgeting rules and regulations in the Town's charter. The financial reports that were being produced were materially misstated.

Cause – The Town changed accounting systems and financial management simultaneously. This uncovered a number of issues in the existing accounting practices.

Recommendation – Written financial reporting procedures must be developed for the new system. A checklist of monthly closing procedures should be prepared and deadlines set to assure timely and accurate financial reporting.

Views of Responsible Officials and Planned Corrective Actions – The current financial management has balanced the records for the year ended June 30, 2012 and has made substantial changes and improvement for the fiscal year ending June 30, 2013 to assure that these issues will be resolved.

Specific Situations Leading to the Material Weakness:

Set up of Accounting System

The Town set up a new accounting system early in 2011-2012. There were several significant issues where the automatic downloads into the accounting system were not set up properly:

Cash for Tax Collections

Tax collections were programmed to increase the general ledger's bank balance when they were received by the tax collector's system. Generally, for cash and checks, this was before the deposit had been processed and made by the tax collector. For credit cards and on-line payments, this was sometimes after the deposit had been credited.

There was no correlation between the recording of transactions in the general ledger and the actual deposits into the General Fund bank account. This caused the accounting records to be inaccurate and reconciliations difficult to impossible.

Material Weakness and Significant Noncompliance (Continued)

Specific Situations Leading to the Material Weakness (Continued):

Recommendation: The Town should use the intermediary account that is set up in the computer to post the tax collections. This should be reconciled to the tax collection bank account on a timely basis.

Cash for Payroll Transactions

Payroll transactions were being posted directly from the payroll company's totals to the general ledger cash account. The transactions differed from the actual cash transactions because of voided checks, re-issued checks and other issues. This caused the accounting records to be inaccurate.

Recommendation: The Town should use a clearing account to post the payroll transactions. This would isolate the differences and require appropriate adjustment to be made each pay period.

Lack of a Monthly Closing

The Town does not have a system set up for a monthly close of the accounting records. Such a system would require each balance sheet account to be reviewed and reconciled to supporting documentation. Significant issues that would have been caught and corrected on a timely manner would have included:

- Double Posting of Tax Collections - Five months of worth tax collections were posted into the accounting system twice. This was not noted and corrected on a timely basis.
- Payroll Accruals – Payroll was accrued for three separate funds as of June 30, 2011. The total accrual for the three funds was all reversed on July 1, 2011 to the General Fund. This was not noted and corrected on a timely basis.
- Police Overtime – Certain police overtime is posted directly to accounts receivable even if it will not be billed. This was not noted and corrected on a timely basis.
- Interfund Balances – Interfund balances did not balance. This was not noted and corrected on a timely basis.

Recommendation: A checklist should be developed for the monthly closing process. This would include reconciling each balance sheet account.

Material Weakness and Significant Noncompliance (Continued)

Specific Situations Leading to the Material Weakness (Continued):

General Fund

Bank Accounts

While the bank accounts were being reconciled monthly, the reconciliations were not being used to correct errors in the accounting system. Instead, Excel spreadsheets were developed that would document the cumulative differences between the transactions posted in the accounting system and the bank statement. In some bank accounts these reconciling items were millions of dollars.

This system would isolate large errors or erroneous postings by the bank, but did not correct the posting to the accounting system. In a double entry system, the cash balances in the accounting reports were at time incorrectly reported by millions of dollars, but the misstate in the revenues and/or expenditures were also misstated by equal amounts.

This appears to be how the bank reconciliations had been done for multiple years.

The June 30, 2012 financial statements were corrected for these misstatements.

Recommendation: The bank accounts should be reconciled in the accounting program and all corrections made in the accounting system in a timely manner. The final reconciliation should generally just show reconciling items for deposits that the bank had not posted yet and checks that had not cleared the bank yet. The reconciled balance should equal the amount posted in the general ledger.

Accounts Receivables (non-tax)

There are a number of subsidiary ledgers and systems used to record and track receivables. Receivables were not being reconciled to subsidiary ledgers and systems on a regular and timely basis.

It appears that there has not been a system to reconcile these accounts receivables in years prior to the installation of the new accounting software.

The June 30, 2012 financial statements were corrected for these misstatements.

Recommendation: Receivables should be reconciled on a monthly basis. Periodic statements should be sent to, not only expedite the collection of the receivables, but also as a function of internal control. This should be included on a month end closing checklist noting the following was done and the initials of who did it:

- Reconciled the total on the trial balance to the detailed listing of receivables
- A statement was sent to each of the debtors on the detailed listing
- Documentation of the detailed listing is filed in the finance department

Material Weakness and Significant Noncompliance (Continued)

Specific Situations Leading to the Material Weakness (Continued):

Accrued Expenses

In the prior year, certain budgeted appropriations were not fully expended. An entry was posted to increase the expenditure amount to the appropriation amount. The other side of the entry was posted to "accrued expense". The accrued expense account would indicate that the town was indebted to an outside party.

In the current year, the Town's books had current expenditures posted to the accrued expense account. These were expenses that were incurred in this fiscal year and not accrued expenses as of June 30, 2011.

This practice would allow appropriations to "carry over" from one year to the next without the proper approvals. This is discussed further in the significant noncompliance detail later in Addendum A.

This caused the Town's accounting records to understate the expenditures during the current year.

We did not review prior years to see how long this practice has been occurring.

The June 30, 2012 financial statements were corrected for these misstatements.

Recommendation: Accrued expenses should be reconciled monthly to actual liabilities that have already been incurred. The General Fund's budget is for one fiscal year. It ends on June 30th. The processes set up in the Town's charter must be used to carryover expenditures from one year to the next.

Reserves

The accounting records had a number of "reserves" set up for various purposes at June 30, 2011. These were included in the Town's records as equity that was earmarked for the purpose indicated. This is the proper treatment for equity if it has been appropriately approved to be segregated for the earmarked purposes.

In the June 30, 2011 financial statements, the reserves were reported as liabilities. A liability is a debt owed. Reserves are not a liability. Reserves are equity that is earmarked. It is unclear how this was changed between the Town's records and the prior years' audits.

In addition, revenues and expenditures were posted to the reserves. This caused the revenues and expenditures on the income statement to be underreported.

It appeared that this is how the reserve accounts were treated for multiple years.

The June 30, 2012 financial statements were corrected for these misstatements.

Material Weakness and Significant Noncompliance (Continued)

Specific Situations Leading to the Material Weakness (Continued):

Recommendation: The final accounting records of the Town should be reconciled with the draft of the audit to determine that they are in agreement. In addition, all revenues and expenditures must flow through the income statement (and therefore be included in the budget). No revenue or expenditure should be posted directly to the reserve account.

Reconciliation to the Board of Education

The Town's accounting system reports the total expenditures against the Board of Education budget. The Board of Education's finance department keeps the subsidiary journal. The Town reconciled the total expenditures to the Board of Education expenditures on an Excel spreadsheet. The differences found between the two, although shown on the Excel spreadsheet, were never recorded into the Town's accounting system.

Recommendation: If the Excel spreadsheets that have been developed over the years may help in the reconciliation, but the final step in the monthly reconciliation should be to make sure that the total expenditures shown in the Town's accounting system equal the total expenditures reported in the Board of Education's detailed expenditure report.

Educational Grants Fund

The Board of Education receives and spends a number of educational grants. Most of these grants are state and federal programs. The transactions for these grants are included in the Educational Grants Fund. In addition, the Town receives reimbursements for expenditures. The most significant of these reimbursements is for excess special education costs. For a number of years, the expenditures have been made out of the General Fund and the reimbursements have been recorded in the Educational Grants Fund. This has overstated the expenditures in the General Fund.

In addition, this reimbursement has been treated incorrectly in the Educational Grants Fund. Instead of showing it as grant revenue, it has been recorded as a liability called "deferred revenue". This would indicate that the revenue has not yet been earned. Because this is a reimbursement grant, it is earned before it is even received. The total that had accumulated over the years equaled approximately $4,500,000.

The June 30, 2012 financial statements were corrected for these misstatements.

Material Weakness and Significant Noncompliance (Continued)

Specific Situations Leading to the Material Weakness (Continued):

Recommendation: The Educational Grants Fund is made up of a number of grants. It is important for the Board of Education to track not only the totals in the fund, but also the details of the individual grant. The accounting records should be able to give an allocation of the fund, by grant, at regular intervals.

In addition, we recommend that the Board of Education match the reimbursement for expenditures with the original expenditures. Generally, this would be done in the General Fund. The State Statutes specifically discuss how to do this for the Excess Cost Grant.

Nonmajor Special Revenue Funds

Sewer Taxing District

Accounts Receivables (non-tax) - Receivables were not being reconciled to subsidiary ledgers and systems on a regular and timely basis.

The June 30, 2012 financial statements were corrected for these misstatements.

Recommendation: Receivables should be reconciled on a monthly basis. Periodic statements should be sent to, not only expedite the collection of the receivables, but also as a function of internal control. This should be included on a month end closing checklist noting the following was done and the initials of who did it:

- Reconciled the total on the trial balance to the detailed listing of receivables
- A statement was sent to each of the debtors on the detailed listing
- Documentation of the detailed listing is filed in the finance department

Reserves - Like the General Fund, the accounting records had a number of “reserves” set up for various purposes at June 30, 2011. These were included in the Town’s records as equity that was earmarked for the purpose indicated. This is the proper treatment for equity if it has been appropriately approved to be segregated for the earmarked purposes.

In the June 30, 2011 financial statements, the reserves were reported as liabilities. A liability is a debt owed. Reserves are not a liability. Reserves are equity that is earmarked. It is unclear how this was changed between the Town’s records and the prior years’ audits.

In addition, revenues and expenditures were posted to the reserves. This caused the revenues and expenditures on the income statement to be underreported.

It appeared that this is how the reserve accounts were treated for multiple years.

Material Weakness and Significant Noncompliance (Continued)

Specific Situations Leading to the Material Weakness (Continued):

The June 30, 2012 financial statements were corrected for these misstatements.

Recommendation: The final accounting records of the Town should be reconciled with the draft of the audit to determine that they are in agreement. In addition, all revenues and expenditures must flow through the income statement (and therefore be included in the budget). No revenue or expenditure should be posted directly to the reserve account.

School Lunch Fund

Receivables – The Board of Education is working to track the costs of catering for school events, self-funding free and reduced meals, and offering free meals to custodians. To accomplish this, the Board of Education has been recording receivables for amounts which are never expected to be received.

It appears that this has been the treatment of these items for multiple years. In prior years, these were removed by the auditor but never corrected in the Board of Education's records.

The June 30, 2012 financial statements were corrected for these misstatements.

Recommendation: The final accounting records of the Board of Education should be reconciled with the draft of the audit to determine that they are in agreement. Where they are not in agreement, the differences should be discussed so corrections can be made to the accounting treatment in a timely manner.

Special Projects Fund

The Town collects grants and donations for special projects. Although these were accounted for by the Town, they were included in the prior audit reports as "Agency Funds". Agency Funds are used to account for money the Town is holding on behalf of others. They are not used to account for money that can be spent for the benefit of the Town.

Recommendation: We recommend that the Town change the treatment of these funds to "Special Revenue Funds". Special Revenue Funds are used to account for revenue restricted for special purposes.

Addendum A

Material Weakness and Significant Noncompliance (Continued)

Specific Situations Leading to the Material Weakness (Continued):

Enterprise Funds

Enterprise funds are required to use the full accrual basis of accounting similar to the accounting that businesses use. Although the prior year audits stated that the enterprise funds were using the full accrual basis of accounting, the Funds' capital assets and long-term debt were not posted to these funds. Instead, capital expenditures and principal payments on long-term debt were expensed.

Recommendation: Capital assets and long-term debt related to the Enterprise Funds should be properly recorded in the Enterprise Funds.

Specific Situations Leading to the Material Noncompliance (Continued):

MNC-2012-01 – Compliance with Budget Rules and Regulations

Criteria – The Town's Charter makes provisions for additional appropriations and transfers to budgeted expenditures so that the actual expenditures do not exceed the approved budget.

Condition – The Town did not have timely and accurate financial reporting for the fiscal year (see material weakness number MW-2012-01). This prevented management from appropriately monitoring the budget.

Effect – A number of budgeted expenditures are over expended.

Cause – The Town changed accounting systems and financial management simultaneously. Interim internal financial reporting became inadequate.

Recommendation – Accurate and timely financial reporting must be reviewed and analyzed to assure that adequate balances are in the budget prior to making new commitments.

Views of Responsible Officials and Planned Corrective Actions – The 2012 and 2013 year to date financial reporting was updated and balanced simultaneously. Appropriate budget adjustment will be made for 2013 before the end of the year. By 2014, appropriate budgets will be in place prior to making commitments against them.

Material Weakness and Significant Noncompliance (Continued)

Specific Situations Leading to the Material Non-Compliance:

Uncommitted Appropriations for Capital Improvements

Section C5-28(B) of the Town's Charter states "all uncommitted appropriations for capital improvements may, at the end of any fiscal year, with the approval of the Board of Finance, be continued and set up as reserve for the same purposes and may be committed by the Board of Finance for the same capital improvements for one fiscal year after the expiration of the fiscal year for which such appropriations were made".

There is no indication that the capital projects carried from fiscal year 2011 into 2012 were approved by the Board of Finance. In addition, the expenditures related to the capital projects was paid directly out of the reserve fund and not shown on the income statement. This has caused the expenditures to exceed the approved budget.

Recommendation: If capital expenditure are not expended or encumbered at the end of the year, management should request that the Board of Finance carry them over to the next fiscal year in accordance with Section C5-28 of the charter. If approved, the accounting records would:

- Assign a portion of the General Fund's Fund Balance at the end of the year for the approved capital improvement. This amount would be equal to the amount that was approved by the Board of Finance, and

- Record the amount carried over as an additional appropriation in the budget for the next fiscal year. All expenditures must then be posted to the income statement. No revenues or expenditures should be posted directly to reserve accounts.

Over-expended Appropriations

Section C5-29 of the Town's Charter states "Neither the Town Council nor any officer, board, commission or committee shall expend any money or enter into any contract for any purpose by which the Town shall become liable for any sum which, with any contract then in force, shall exceed the sum appropriated by the Town for such purpose, except in cases of necessity connected with the repair of public buildings, sewers, sewage disposal plants, highways and bridges and with public welfare, and then not to exceed the amount provided by § 7-348 of the General Statutes."

Section 7-348 of the Connecticut General Statutes states "No officer of such town shall expend or enter into any contract by which the town shall become liable for any sum which, with any contract then in force, shall exceed the appropriation for the department, except in cases of necessity connected with the repair of highways, bridges, sidewalks and water and sewer systems and the care of the town poor, and then not more than one thousand dollars."

Addendum A

Material Weakness and Significant Noncompliance (Continued)

Specific Situations Leading to the Material Non-Compliance (Continued):

A number of appropriations were over expended. Some of these were over-expended because of necessity with two major storms. Some of these were over-expended because management did not have adequate interim reporting.

Recommendation: Timely and accurate interim reporting must be prepared for management. The requirements of the Town's Charter must be followed. At the next Charter revision, consideration should be given to increasing the amount that could be spent in an emergency such as a significant hurricane or large snow storm.

Town of New Canaan, Connecticut

Addendum B

Observations/Recommendations: Internal Control and/or Operating Efficiency

Discussion of Significant Cycles

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.

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. We would recommend that this include at least:

- Periodic 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.

General Government – Non-Payroll Transactions

Budget vs. Actual Reporting

There is no budget vs. actual report prepared for management and board members on a regular basis. Decisions must be made without enough timely and accurate information.

Recommendation: A timely and accurate budget vs. actual report and a balance sheet should be prepared, balanced, and distributed monthly.

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

Discussion of Significant Cycles (Continued)

Nonpayroll Disbursements

The senior accountant holds the blank check stock. She also prints the checks with the Treasurer's electronic signature. The senior accountant also reconciles the bank statement.

Recommendation: Controls must be put in place to prevent the senior accountant from printing unauthorized signed checks and to detect, in a timely manner, if this is done.

Credit Cards

The Town has a number of credit cards issued in its name. The Town does not have a listing of which credit cards have been issued, who holds them and the spending limit on each card.

Recommendation: The Town should have such a listing.

Receiving Reports

The Town does not require receiving reports to indicate goods purchased were actually received. This is combined with the invoice authorization. Sometimes the invoice is approved by individuals that would not have received the goods.

Recommendation: We recommend that the Town consider using receiving reports as part of their invoice approval process.

Encumbrances

The Town allows encumbrances to be recorded against the budget in the year that the encumbrance was made. Encumbrances are firm commitments, evidenced by a signed agreement or binding purchase order, made as of June 30th. We noted that there was a liability for Encumbrances that had been carried over for multiple years. This would indicate that it was either not reconciled for a number of years or not a binding commitment.

Recommendation: We recommend that the Town develop a policy for encumbrances. The lack of a specific definition in authoritative literature could lead to what might seem like budget manipulations. A policy defining what is acceptable as an encumbrance could offset that.

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

Discussion of Significant Cycles (Continued)

General Government – Payroll Transactions

Payroll Register

The details for the paychecks are inputted into the computer system by the payroll clerk. This information generates individual paychecks as well as a summary journal entry. The summary journal entry is reviewed by someone other than the payroll clerk, but the individual paychecks are not. It is possible that an individual paycheck could be in error or posted more than one time.

Recommendation: The payroll register, showing the details of gross pay, withholdings and net pay and totaling the journal entry should be reviewed by someone other than the payroll clerk.

Education – Non-Payroll Transactions

Bidding

The Board of Education's policy encourages bidding for high value items, but bidding is rarely done.

Recommendation: We recommend that the Board of Education establish a bidding policy with a specific dollar amount and acceptable exceptions. In addition, the Board of Education should note how to make exceptions to the policy in rare circumstances.

Encumbrances

The Board of Education allows encumbrances to be recorded against the budget in the year that the encumbrance was made. Encumbrances are firm commitments, evidenced by a signed agreement or binding purchase order, made as of June 30th. We noted items in encumbrances that, with a proper policy, might not be considered encumbrances.

Recommendation: We recommend that the Board of Education develop a policy for encumbrances. The lack of a specific definition in authoritative literature could lead to what might seem like budget manipulations. A policy defining what is acceptable as an encumbrance could offset that.

Credit Card Transactions

The Board of Education Finance Director holds one of two credit cards that are approved. Although the authorized limit on the credit card is only $3,000, the Finance Director approves his own credit card use.

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

Discussion of Significant Cycles (Continued)

Recommendation: We recommend a separate individual approve the Finance Director's credit card bills.

Signatures on Checks

A device is attached to the printer to prevent checks being printed without proper authorization. A signature card is required to be inserted into the device in order to allow the signatures to be printed. However, the signature cards are never removed. The device is located next to the printer and is in not was locked or secured.

Recommendation: We recommend that the signature cards be removed when not needed and that the controls over printing signed checks be reviewed.

Old Outstanding Checks

The Board of Education has some outstanding checks on their bank reconciliation that are up to 10 years old.

Recommendation: These should be reviewed to determine if they are really outstanding checks or errors. If they are indeed outstanding checks, the State's unclaimed property procedures should be implemented as applicable.

Education –Payroll Transactions

The Board of Education is deducting certain payroll withholding amounts in pre-tax dollars. The Board of Education does not have a written IRS Section 125 plan which is required for this treatment.

Recommendation: We recommend that the Board of Education have a written IRS Section 125 plan.

Other Items

Board of Education - Educational Grants Accounting and Reporting

The Board of Education is required to send annual reports to the State for certain State and federal grants. When the grant is not fully expended, the can be carried over to the next year. Instead of going through the procedures with the State for carrying the grants over, the Board of Education recorded an expenditure for the unspent portion of the grant to carry over the grant without proper State authorization.

Recommendation: We recommend that the Board of Education follow the appropriate State process for carrying over these grants and proper reporting on Form ED141.

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

Other Items (Continued)

Ethics Policy for Disclosure of Interest in Transactions

Section 17-5E of the Town's Code of Ethics states "Every person who is an employee or an elected or appointed official of the Town of New Canaan, including the Board of Education (collectively, the "town"), shall file with the Town Clerk, on forms provided for such purpose, a signed statement disclosing any known transaction with the town involving the procurement of real property, goods or services in which such person or spouse, child or dependent of such person holds a financial interest as an individual or as an employee of or as a partner or at least a five-percent shareholder in, a participating entity."

Although they are being filed now, these forms were not originally filed on a timely basis.

Recommendation: We recommend that the Town follow the provisions of the Code of Ethics. In addition, we recommend everyone to whom it applies get ethic's training when they first become subject to the Code and then every 2 years. In addition, the Code of Ethics should be a "live document". It should be reviewed on a regular basis for possible additions and amendments.

Capital Expenditure Budgets

The Town approved certain expenditures for the Lake Avenue Bridge. As the original budget was reached, the project did not come back to the Board of Finance and Town Council for an additional appropriation in a timely manner.

Recommendation: The finance should prepare project length budget versus actual reports for each of the capital projects. These should be reviewed with management on a regular basis so the budget can be monitored.

Capital Leases

The Board of Education financed certain capital equipment with capital leases in previous years. Although the lease was recorded as long-term debt, the related capital assets were not all capitalized.

Recommendation: A checklist should be prepared to review the depreciation schedules at the end of the year. This should include assuring that capital leases are added.

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

Other Items (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.

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

Town of New Canaan, Connecticut

Addendum C

Information Technology Observations and Recommendations - General Government

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.

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. The administrators of the system are capable of modifying the approval workflows for disbursements. 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.

Information Technology Observations and Recommendations - General Government (Continued)

Network Folder Access Rights

We reviewed a selection of network folders used by the Town to verify that access is appropriately assigned and unauthorized access is prevented. Failure to monitor access to sensitive network folders can result in unauthorized access, use, modification, and/or destruction of information.
In our review of the access restrictions, we identified that the personal network folder of the Chief Financial Officer was incorrectly restricted. Any employee with valid network credentials could gain access to the folder. However; the CFO had yet to store any data in the folder. The issue was immediately addressed and access was restricted to only the CFO.

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 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.

Active Directory

Active Directory is the directory service used by the Town 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:

Password Management

We reviewed the design and implementation of the password controls of the Town to ensure that controls in operation would reasonably protect against unauthorized access to system and network resources. Active Directory passwords are also used to gain access to the primary financial system. As such, strong Active Directory passwords are critical in providing assurance of the integrity of the data within the financial system. We noted the following:

- No programmatic control has been implemented to require password complexity. Password complexity is defined as a password that contains a combination of upper and lower case letters, numbers, and special characters (i.e. #$@%^&*!). As such, employees would not be prevented from selecting trivial passwords such as “password” or “12345678”.

- The Town has implemented a password expiration policy; however, we identified a large number of employees that were excluded from the policy. A set of these employees have transactional access to the financial system.

Information Technology Observations and Recommendations - General Government (Continued)

We recommend that the Town implement a programmatic control that will require all passwords selected to meet the complexity requirements noted above. In addition, we recommend that all employees are subject to the password expiration requirement. Exclusions should only be authorized after an analysis of the potential risk and Town defined exclusion criteria has been met. A series of compensatory controls should be implemented to offset any increased risk.

Administrative Account Sharing

We noted during our review that the default Active Directory "administrator" account is shared between members of the IT Department. Because the account is shared, actions performed by the account cannot be directly linked to a specific individual. Because of the level of privilege assigned to these accounts it is critical that the Town have the ability to hold specific employees or vendors accountable for their actions. This type of accountability can help deter unethical and/or fraudulent activity.

We recommend that all administrative employees are required to perform administrative functions with uniquely assigned administrative accounts. This will ensure a proper trail of accountability for actions performed.

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 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 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.

Information Technology Observations and Recommendations - General Government (Continued)

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
- Logon Events
- 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 Town (e.g. the prior 60 days etc).

Service Account Management

Service accounts are network accounts that are used to allow a service (i.e. a program) to execute with a defined set of security permissions. Failure to properly control service accounts can result in unauthorized access to system, network and information resources.

We noted that service accounts were configured with passwords that were not set to expire and certain service accounts were granted domain administrator privileges. In addition, we noted that a standard was not defined for the creation of the service accounts, such as password complexity.

We recommend that the Town develop a set of guidelines that will govern all service account creation. As additional guidance, we offer the following best practice guidelines regarding service account management:

- Service account passwords should be created with significant complexity. This can be defined as 30+ characters in length with characters consisting of upper and lower case letters, numbers, and special characters (i.e. ! @ #, etc). Because service account passwords are typically not changed as frequently as user accounts, the use of a significantly complex password will offset the risk of not changing that password frequently.

- Service account passwords should be changed at least once yearly.

- Service accounts should be assigned the least privileges possible to execute only their intended function (e.g. read, write, execute, etc.).

- Where possible, service accounts should have their access restricted to only the systems for which they will need to access.

- Service accounts should never be assigned to an Active Directory privileged group (e.g. Domain Administrators) unless absolutely necessary.

Information Technology Observations and Recommendations - General Government (Continued)

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, all other terminations may not be communicated on a timely basis. As a result, a terminated employee account can remain active for a period of time after the official termination date.

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 Town IT assets.

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 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.

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.

Information Technology Observations and Recommendations - General Government (Continued)

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 periodically test this plan for functionality as well as practicality.

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.

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.

Information Technology Observations and Recommendations - General Government (Continued)

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 Town 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 communications to only those required for Town operations.

We recommend that the Town increase their level of restrictiveness on its firewall and only allow the communications necessary for the Town to maintain operations. In addition, access rules on the firewall should be reviewed once annually to ensure that the access rules are accurate and relevant for the Town's operations.

Network Device Management

Network devices, such as switches and routers, function as the core mechanisms by which data is transmitted through the Town network. Without such devices systems and applications would be unable to communicate with one another. Failure to adequately secure and manage these devices can result in network downtime and/or the unauthorized access, use, modification, and or destruction of information resources.

We noted during our review the following:

- SNMP Management Protocol was configured in read and write mode.
- Management protocol passwords in the configuration were unencrypted.
- Telnet is utilized to connect to the devices instead of SSH.

We recommend the following:

- SNMP protocol is restricted to read only.
- Management protocol passwords are encrypted in the configuration file.
- SSH is exclusively used for the remote management of network devices.

Addendum D

Information Technology Observations and Recommendations - Education

IT General Control Assessment

We assessed the Information Technology "IT" general controls of the Board of Education's ("BOE") systems and applications to ensure that policies, procedures, and operational practices were implemented to help support the BOE'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 BOE does not have a comprehensive set of documented standard operating 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 BOE 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.

ADP Payroll

We interviewed the person responsible for payroll to gain an understanding of the general controls within the ADP application. We noted that the person currently responsible for payroll is the only employee with knowledge of the payroll application passwords. Should that employee be unavailable to process payroll, the BOE is at risk of being unable to satisfy their payroll liabilities. In addition, we noted that the password used to access the payroll application is not changed on a periodic basis.

We recommend that the BOE formally designate an employee as the backup payroll processor. The assigned employee should be provided with the credentials necessary to carry out the payroll function. In addition, the application passwords should be changed every 60 -90 days.

Information Technology Observations and Recommendations – Education (Continued)

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. Access included, but was not limited to, the ability to modify the general ledger chart of accounts and in one instance; an employee was assigned user security access. User security access allows the modification of user access assignments in the application. 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 BOE 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.

Network Folder Access Rights

We reviewed a selection of network folders used by the BOE to verify that access is appropriately assigned and unauthorized access is prevented. Failure to monitor access to sensitive network folders can result in unauthorized access, use, modification, and/or destruction of information.

We identified a human resource's departmental folder and a set of personal network folders that were incorrectly restricted. Any student or employee with valid network credentials could gain access to these folders. We noted that the issue is a known issue and is scheduled to be corrected.

We recommend that the BOE conduct a formal assessment of all network folders to ensure access is appropriate.

Recertification of Access Rights

The BOE 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 BOE 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.

Information Technology Observations and Recommendations – Education (Continued)

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 BOE 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 BOE 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 BOE 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 BOE are significantly weak. We 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.

- The BOE has implemented a remote access technology that uses Active Directory credentials to obtain access. This remote access technology is accessible from the internet using a standard web browser.

Information Technology Observations and Recommendations – Education (Continued)

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.

Inappropriate Employee Membership in Active Directory Privileged Groups

Membership in an Active Directory privileged group can grant those members with unrestricted access to the entire Windows network, including the ability to modify network security and alter network user access. Access to this group can intentionally or unintentionally facilitate disruptive, unethical, and/or fraudulent activities. To ensure the security, integrity and availability of the environment it is critical that access to this group is strictly limited, controlled, and monitored.

In our review of the members of the privileged groups, we observed a set of employees for which we could not identify a business reason for membership. The employees identified consisted of help desk technicians and non IT employees. The help desk technicians were granted membership to carry out their day to day functions; however, the access rights inherited from this membership are in excess of their assigned responsibilities. We did not identify a justification for the non IT employees. We noted that the BOE has hired an outside consulting firm to help them this issue.

We recommend that membership in the privileged groups are adjusted to contain only approved IT personnel as soon as possible. Help desk technicians should only be delegated the permissions necessary to perform their assigned responsibilities. In addition, we recommend that the Active Directory privileged groups are reviewed semi annually by IT management to ensure access remains accurate and relevant.

Information Technology Observations and Recommendations – Education (Continued)

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 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 BOE 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 BOE consistently audit the following events for both successes and failures for all workstations and servers:

- Account Logon Events
- Logon Events
- 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 BOE (e.g. the prior 60 days etc).

Service Account Management

Service accounts are network accounts that are used to allow a service (i.e. a program) to execute with a defined set of security permissions. Failure to properly control service accounts can result in unauthorized access to system, network and information resources.

Information Technology Observations and Recommendations – Education (Continued)

We noted that service accounts were configured with passwords that were not set to expire and certain service accounts were granted domain administrator privileges. In addition, we noted that a standard was not defined for the creation of the service accounts, such as password complexity.

We recommend that the BOE develop a set of guidelines that will govern all service account creation. As additional guidance, we offer the following best practice guidelines regarding service account management:

- Service account passwords should be created with significant complexity. This can be defined as 30+ characters in length with characters consisting of upper and lower case letters, numbers, and special characters (i.e. ! @ #, etc). Because service account passwords are typically not changed as frequently as user accounts, the use of a significantly complex password will offset the risk of not changing that password frequently.
- Service account passwords should be changed at least once yearly.
- Service accounts should be assigned the least privileges possible to execute only their intended function (e.g. read, write, execute, etc.).
- Where possible, service accounts should have their access restricted to only the systems for which they will need to access.
- Service accounts should never be assigned to an Active Directory privileged group (e.g. Domain Administrators) unless absolutely necessary.

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, all other terminations may not be communicated on a timely basis. As a result, a terminated employee account can remain active for a period of time after the official termination date. During our testing of the termination process, we identified a series of active accounts for terminated employees. In addition, we noted that the records of IT assets assigned to the employees are stored with the IT department and not human resources. As a result, there is a risk that BOE assets may not be collected as part of the termination process should IT not be notified.

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 BOE IT assets.

Information Technology Observations and Recommendations – Education (Continued)

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 noted that all users are configured with local administrator access to their machines. We noted this is the result of vendor application requirements.

While we recognize that certain applications may require elevated privileges for proper operation, typically the assignment of full administrative access can be avoided. Application vendors in most cases 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 BOE, 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 during our review that no technical control has been implemented to force the systems to lock after a specified period of inactivity. An unattended and logged on workstation is the equivalent of an openly available user ID and password.

We recommend that a control mechanism is implemented to lock the workstations after an idle period of 15 to 30 minutes. This control should be implemented in a manner that prevents the end users from manipulating or disabling the control.

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 BOE 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.

Information Technology Observations and Recommendations – Education (Continued)

We recommend that the BOE 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 BOE 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:

- A folder used by the Administrators of the schools was not included in any of the backup jobs. This folder was immediately selected for inclusion upon discovery.
- No documentation exists that explicitly outlines what is to be included for backup. Without such, there can be no validation of the backup selections and no change control mechanism to identify deviations from the approved configuration baseline.
- No formal procedure exists to validate the integrity of the backed up data through the implementation of scheduled data restoration testing.

We recommend that the BOE develop an authoritative document for all backup selections. Any changes to the backup selections should occur through the change control process and the changes reflected in the master documentation. In addition, 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 BOE 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 BOE to perform in the event of a disaster, the BOE is at risk for failure to successfully and quickly recover.

We recommend that the BOE 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.

Information Technology Observations and Recommendations – Education (Continued)

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 BOE does maintain a central antivirus system, we noted the following:

- The password used to access the BOE antivirus administration console was the vendor default password.

- A safeguard does not exist to issue e-mail alerts to the IT employees 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 BOE's systems and networks.

- A large number of workstations were significantly behind in antivirus signature updates. The workstations included those used by finance personnel with privileged access to the Munis system and payroll application.

We recommend that the BOE implement a mechanism to immediately alert the IT employees if a virus is detected and not removed. The antivirus administration console should be monitored on a daily basis to identify any workstations that are out of date. Any workstation identified should be investigated and the issue corrected in a timely manner. Independent of the antivirus administration console, it is best practice to change vendor defaults for all applications prior to deployment into a production environment.

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 BOE 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.

Information Technology Observations and Recommendations – Education (Continued)

We noted in our review of the firewall configurations that the firewall is not configured to restrict outbound communications. In addition, we noted that inbound traffic rules from the internet are not periodically reviewed and assessed to ensure that the rules are accurate and relevant. As such, during our review, we identified a rule set that was not needed.

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

Network Device Management

Network devices, such as switches and routers, function as the core mechanisms by which data is transmitted through the BOE network. Without such devices, systems and applications would be unable to communicate with one another. Failure to adequately secure and manage these devices can result in network downtime and/or the unauthorized access, use, modification, or destruction of information resources.

We noted the following:

- Default device passwords have not been changed.
- SNMP Management Protocol was configured in read and write mode.
- Management protocol passwords in the configuration were unencrypted.
- Telnet is utilized to connect to the devices instead of SSH.

We recommend the following:

- A complete security assessment of all network devices is conducted as soon as possible.
- Passwords are changed as soon as possible.
- SNMP protocol is restricted to read only.
- Management protocol passwords are encrypted in the configuration file.
- SSH is exclusively used for the remote management of network devices.