TOWN OF CHELMSFORD, MASSACHUSETTS

MANAGEMENT LETTER

JUNE 30, 2019

To the Honorable Board of Selectmen
Town of Chelmsford, Massachusetts

In planning and performing our audit of the financial statements of the governmental activities, the business-type activities, each major fund, and the aggregate remaining fund information of the Town of Chelmsford as of and for the year ended June 30, 2019, in accordance with auditing standards generally accepted in the United States of America, we considered the Town's internal control over financial reporting (internal control) as a basis for designing our auditing procedures 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.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies, and, therefore, material weaknesses or significant deficiencies may exist that were not identified.

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. We did not identify any deficiencies in internal control that we consider to be material weaknesses.

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. We did not identify any deficiencies in internal control that we consider to be significant deficiencies.

However, during our audit we became aware of other matters that are opportunities for strengthening internal controls and enhancing operating efficiency. The memorandum that accompanies this letter summarizes our comments and suggestions concerning those matters.

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

Powers & Sullivan LLC

October 1, 2019

TOWN OF CHELMSFORD, MASSACHUSETTS

MANAGEMENT LETTER

JUNE 30, 2019

TABLE OF CONTENTS

Current Year Comments

FRAMEWORK FOR ASSESSING AND IMPROVING CYBERSECURITY

<u>Current Year Comment</u>

Throughout an organization's normal course of business comes the need to collect, transmit, and store extensive amounts of personal and financial information, both in paper and electronic form, relating to residents, vendors and employees. The use of technology has become a driver in helping organizations stay current and succeed. However, the sharing and compilation of this information lends itself to increasing the organization's vulnerability to either a cyber computer attack, ransomware attack, or a security breach, all are considered cybersecurity attacks.

Management must be aware of the risks associated with the collection of this information and be diligent in implementing the proper policies and procedures to help to expose these risks. While impossible for an organization to eliminate all risks associated with a cybersecurity attack, an organization can take a variety of steps to mitigate its exposure, satisfy its governance responsibilities and help to minimize the impact of any attack occur.

Because management is ultimately responsible to develop, implement and operate an organization's cybersecurity risk management program, management is ultimately responsible for developing, and presenting to the organization an overview of the entity's cybersecurity risk management program.

The first step in understanding an organization's risks and working to develop and implement an effective cybersecurity plan, an organization needs to conduct a risk assessment and understand their where its greatest exposure and vulnerabilities lie. This can be completed internally if the organization has an experienced information technology team, or there are many organizations that employ experienced professionals in the information technology arena to assist in the risk assessment and implementation if desired.

Once a risk assessment is completed, the next step is to develop and implement a cybersecurity risk program which needs to be continually reviewed and updated as technology changes. This response program should be tested to determine if the proper policies and procedures have been implemented to minimize the potential costs of a cyber-attack.

The obvious benefit to conducting a risk assessment is having the knowledge and an objective identification of the organization's areas where exposure to risks is more prevalent and allows for the development of a roadmap to address the remediation of these risks.

Some of the main areas of review that should be incorporated into the risk assessment are as follows:

- Electronic Records, Paper Records (Human Resource Records, Bank Statements, Payroll Records), Resident Data, Employee Data, Physical Security of hardware and software, Any Third Party or Vendor exposure, Password Security, E-Mail Security (Understanding the risks of malware and ransomware), Mobile phones and Portable Storage Devices, System Backup Procedures, Virus Protection Software, Data Encryption, Document Retention and Destruction Policies, Use of Unauthorized Software, Ongoing Employee Training.

Risk management is the ongoing process of identifying, assessing the risk, and developing a plan to address the risks. In order to manage their risk, organizations should understand what the likelihood is that an event will occur and assess the resulting impact of the event. This will assist the organization in developing their own acceptable level of risk tolerance and help to prioritize the areas in which internal controls should be strengthened.

<u>Recommendation</u>

Per our inquiries with the Town's Information Technology department, the Town is aware of their risk exposure to a cyber-attack and has taken a pro-active approach to mitigate their risk exposure to a cyber-attack. However, we recommend that management formally document the Town's assessment of risk exposure to a cyber-attack. An internal team with the proper information technology experience can be used or a third-party vendor that specializes in this type of assessment can be used.

Once a review is completed, we recommend that policies and procedures be developed to mitigate each identified risk to an acceptable level that fits with the organization's determined risk tolerance.

We also recommend that the community look into obtaining Cyber Liability Insurance which will help to mitigate the costs associated with a breach in information technology security.

Finally, we want to make management aware that technology is constantly changing and that this is not a one-time static process, this will require additional risk assessments and the updating of policies and procedures with the changing technological landscape.

Prior Year Comments

RECONCILATION OF THE HEALTH AND DENTAL INSURANCE BILLS

Prior Year Comment

The Town obtains health insurance and dental insurance through the Massachusetts Interlocal Insurance Association (MIIA). Each month deductions are taken from each employee's paycheck that is enrolled in the health plan, and these deductions are taken a month prior to the applicable insurance coverage month. Furthermore, for retirees, either the Town notifies Middlesex County Retirement of the cost per each retiree, and that cost is deducted from the retirees' retirement benefits, or the retiree pays directly to the Town the cost of their coverage. Each month the Town receives a bill from MIIA indicating the total cost of the insurance, and the bill details the employees that are covered and their plan and coverage type. It is important that each month the information on the bill is reconciled to Town records to ensure that the Town is being billed for the proper employees (active employees and retired employees), the proper plan type, and the proper plan coverage to ensure that the proper deductions are taken from the employees each month. Through our testing and inquires with Town management, we noted that the Town and School's Human Resource Department are responsible for reconciling the health insurance and dental insurance bills from MIIA.

In discussing the Town Human Resource department's process for reconciling we noted that any changes in health insurance and dental insurance plans for an employee is compared to the bills received each month, however a full review of the bill in its entirety is reconciled quarterly. Although this was indicated through inquiry, the procedures performed to reconcile the bills was a manual cross-reference check and was not formally documented and no back-up was provided, therefore we were unable to confirm that these reconciliations were being performed routinely throughout the year.

Additionally, the School Department did not provide us supporting documentation regarding their reconciliation procedures of the health insurance bill to supporting source documentation or to a master database file that is used in compiling the census data that is sent to the actuary.

Current Status

The Town's Human Resource department performed a reconciliation of the Town's health insurance bill to the Town's payroll software matching the employee name and plan-type for the active members. However, as of September 2019 a reconciliation had not been performed since April 2019, and the Town does not have procedures in place to reconcile on a routine basis. Furthermore, we were not provided with any support regarding a reconciliation of the Town's retirees receiving health insurance benefits. Also, the School department did not provide us with supporting documentation regarding their reconciliation procedures of the health insurance bill to supporting source documentation.

Recommendation

We recommend that the Town and School Human Resource departments implement standard, proper, and efficient procedures for reconciling the bills, that these reconciliations are being performed on a periodic basis, and that the procedures performed are properly documented. We also recommend that the Town implement a proper affidavit process to ensure that any retiree that the Town is being billed for is a living retired member currently receiving health benefits.

DOCUMENTATION AND RETENTION OF PERSONNEL FILES

<u>Comment</u>

When an employee enrolls in the Town's health insurance plan, a member enrollment form is completed and turned into the Town's Human Resource department. Furthermore, when an employee is initially hired by the Town, source documentation confirming their date of birth and marital status is reviewed by the Town's Human Resource department. Per our review of health insurance information and support, we noted that the Human Resource department does not properly retain this documentation in an employee personnel file throughout the duration of employment and/or retirement. Proper source documentation should be retained throughout employment or throughout the life of a retiree to ensure that any insurance or retirement benefits being paid or given to employees and any liability associated with pending payments and insurance benefits is properly supported.

<u>Current Status</u>

We selected a sample of school department and non-school employees hired throughout 2019 as well as employees who retired throughout 2019 and requested source documentation confirming their date of birth, marital status, and health insurance enrollment.

Out of the 10 non-school employees selected for our testing, 6 did not have records in their personnel files confirming their date of birth. Additionally, 4 of the health insurance enrollment forms were not properly filled out, of which 3 were also not signed by the employee. We were also not provided with source documentation for 4 members confirming their marital status.

Out of the 10 school employees selected for our testing, 9 did not have records in their personnel files confirming their date of birth. 1 employee did not have a health insurance enrollment form on file and an additional employee had a complete initial enrollment form, but the subsequent form to cancel health insurance was not signed by the employee.

<u>Recommendation</u>

We recommend that for each active employee and for each retiree that is currently receiving health insurance benefits from the Town, the Human Resource department retain a personnel folder containing various source documents and information. The personnel folder should include information regarding the health plan chosen upon enrollment, any subsequent changes to the plan or coverage type, and any personnel documents confirming proof of birth for both the employee and their spouse who is receiving benefits and proof of marriage.

MAINTAINING AND UPDATING HEALTH INSURANCE DATABASE

<u>Comment</u>

Through our inquiries on the process of providing census data information to the Town's actuary in preparation of the Other Post Employment Benefit actuarial valuation, we noted that this process is inefficient. For retirees, the Town receives a file from MIIA and then manually enters in health insurance information for each retiree listed. Not only is this process inefficient, but a manual process increases the risk that information is not entered into the spreadsheet correctly. This spreadsheet is then sent to the Town's actuary to prepare the actuarial valuation.

Current Status

No action was taken in 2019 to maintain a spreadsheet or database detailing the census information and health insurance plan information for each member.

Recommendation

We recommend that the Human Resource department be responsible for enrolling both active members and retirees in the Town's health insurance plans maintain a spreadsheet or database detailing the census information and health insurance plan information for each member. That database should be updated as active members and retirees enroll, withdraw, and change their health insurance coverage. This database should also be supported with source documentation that is contained in a member file folder for each active employee and retiree as detailed in the previous comment. This database should also be used to periodically reconcile the health insurance bills and the health and dental insurance deductions taken monthly from active employees and paid monthly for retirees.