CITY OF SPRINGFIELD, MASSACHUSETTS

MANAGEMENT LETTER

JUNE 30, 2018

Powers & Sullivan, LLC
Certified Public Accountants

100 Quannapowitt Parkway
Suite 101
Wakefield, MA 01880
T. 781-914-1700
F. 781-914-1701
www.powersandsullivan.com

To the Honorable Mayor, the City Council, and Management
City of Springfield, Massachusetts

In planning and performing our audit of the financial statements of the governmental activities, the business-type activities, the aggregate discretely presented component unit, each major fund, and the aggregate remaining fund information of the City of Springfield, Massachusetts as of and for the year ended 2018 (except for the Springfield Contributory Retirement System which is as of and for the year ended December 31, 2017), in accordance with auditing standards generally accepted in the United States of America, we considered the City'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 City's internal control. Accordingly, we do not express an opinion on the effectiveness of the City's internal control.

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

We will review the status of these comments during our next audit engagement. We have already discussed these comments and suggestions with various City personnel and will be pleased to discuss them in further detail at your convenience, to perform any additional study of these matters, or to assist you in implementing the recommendations.

The City's written responses to the matters identified in our audit have not been subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on them.

This communication is intended solely for the information and use of management of the City of Springfield, Massachusetts, and is not intended to be and should not be used by anyone other than these specified parties.

Powers + Sullivan, LLC

November 30, 2018

CITY OF SPRINGFIELD, MASSACHUSETTS

MANAGEMENT LETTER

JUNE 30, 2018

CONTENTS

Current Year Comments

OLD PERSONAL PROPERTY TAXES

Comment

The City is carrying personal property tax balances dating as far back as fiscal year 2000. The total amounts outstanding beyond 2 years old at June 30, 2018 amounted to approximately $13.7 million, of which approximately $10.3 million is due from one utility customer and these amounts are being contested and may not be ultimately collectible. Note that the City has recorded reserves against these balances for financial statement reporting purposes.

Recommendation

We have recommended several times over the years that all concerned parties come together to create financial policies over collection, abatement, and write-offs of these older balances. More recently, the City's Director of Internal Audit prepared similar recommendations that have been submitted to management for consideration. We agree with the City Auditor's recommendations and continued to encourage management to take action on these older outstanding balances.

City's Response

Regarding the delinquent utility account, the Board of Assessors has been collaborating with three other large communities on defending the assessed value and completing the litigation process.

The Board agrees with the finding and will continue to work with the City Collector to abate such requests after completing our due inquiry.

Prior Year Comment - Unresolved

OPERATIONS OF THE FRANCONIA AND VETERAN'S MEMORIAL GOLF COURSES

Previous Comment

The City owns and operates two municipal golf courses primarily for the benefit of City residents. The golf courses are managed by the City's Department of Parks, Buildings, and Recreational Management (DPBRM). The DPBRM has entered into a personal services contract with Ryan Hall's Golf Shop LLC to provide a Golf Professional and staffing necessary to operate the day-to-day activities of the two golf courses. The Golf Professional reports to the Executive Director of the DPBRM. The Personal Services Contract contains numerous responsibilities of both the City and Ryan Hall's Golf Shop LLC that are intended to provide for the overall management of the courses.

There is a significant amount of monitoring required by the DPBRM to ensure that the Contract is adhered to and that the golf courses are operated properly for the benefit of the City and its residents.

Continuing Recommendation

We recommend that City Management and the DPBRM develop detailed procedures to monitor the various aspects of the Contract. All parties involved should agree on the mutual responsibilities included in the Contract and the agreement should be updated periodically to delineate changes as time goes on.

City's Current Response

The City agrees with the finding and has instituted monthly meetings with the Golf Professional to review operations at both Municipal Golf Courses to ensure contract compliance.

Informational Comments

RETIREMENT SYSTEM FUNDED RATIO

Previous Comment

To comply with Massachusetts General Laws, the Springfield Contributory Retirement System (System) must be fully funded by 2040. As reflected in the most recent actuarial valuation (January 1, 2018), the funded ratio for the System was 27% (26.2% in the previous valuation). The funded ratio is the percentage of the accrued liabilities that are covered by assets accumulated to satisfy the liability. The System's ratio ranks among the lowest percentages in the nation. The current funding schedule places the System in a precarious position which could require future borrowing to fully fund the retirement plan.

Continuing Recommendation

We continue to recommend the System adopt a more aggressive funding schedule in order to avoid the need for future borrowing.

City's Current Response

A new funding schedule was adopted by the Springfield Retirement Board in FY18 in response to the recent actuarial valuation. The Schedule has total appropriations increasing 14% in FY19, then 9% each year through FY33, with a final amortization payment in FY34. The new schedule also drops the assumed Investment return from 7.65% to a more conservative 7.40%.

DOCUMENTATION OF INTERNAL CONTROLS

Comment

In December 2013, the U.S. Office of Management and Budget (OMB) issued Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (Uniform Guidance) in an effort to (1) streamline guidance for federal awards while easing the administrative burden and (2) to strengthen oversight over the expenditure of federal funds and to reduce the risks of waste, fraud and abuse.

The Uniform Guidance supersedes and streamlines requirements from eight different federal grant circulars (including OMB Circular A-133) into one set of guidance. Local governments were required to implement the new administrative requirements and cost principles for all new federal awards and to additional funding to existing awards made after December 26, 2014 (fiscal year 2016).

In conformance with Uniform Guidance, the non-Federal entity must: (a) Establish and maintain effective internal control over the Federal award that provides reasonable assurance that the non-Federal entity is managing the Federal award in compliance with Federal statutes, regulations, and the terms and conditions of the Federal award.

These internal controls should be in compliance with guidance in ''Standards for Internal Control in the Federal Government'' issued by the Comptroller General of the United States (the Green Book) and the ''Internal Control Integrated Framework'', issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Management is responsible for internal controls and to see that the entity is doing what needs to be done to meet its objectives. Governments have limited resources and constraints on how much can be spent on designing, implementing, and conducting systems of internal control. The COSO Framework can help management consider alternative approaches and decide what action it needs to take to meet its objectives. Depending on circumstances, these approaches and decisions can contribute to efficiencies in the design, implementation, and conduct of internal control. With the COSO Framework, management can more successfully diagnose issues and assert effectiveness regarding their internal controls and, for external financial reporting, help avoid material weaknesses or significant deficiencies.

The COSO internal control framework must incorporate the 5 major components of internal control, while addressing the 17 principles of internal control that support the COSO framework. Refer to www.coso.org for articles describing the 5 components and their 17 principles in detail.

Management should evaluate and assess the government's internal control system to determine whether: each of the five essential elements of a comprehensive framework of internal control is present throughout the organization; whether each element addresses all of the associated principles; and whether all five elements effectively function together.

Recommendation

We recommend management follow the best practice for establishing and documenting their internal control system using the COSO Internal Control Framework.

FRAMEWORK FOR ASSESSING AND IMPROVING CYBERSECURITY RISKS

Comment

Throughout an organization's normal course of business comes the need to collect, transmit, and store extensive amounts of personal and financial information, in both 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 an attack.

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 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.

Recommendation

We recommend that management continue with its pro-active approach and assess their risk exposure to cyber-attacks. This would include that the City and the School department, through its Information Technology department, phish and train its employees to protect against phishing attacks. There are a number of software packages in the marketplace, some of which are free, which the City can use for such purposes.

Management has initiated several IT audits which were performed by experienced external auditors who specialize in this type of work and has received detailed reports from these audits. 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.

Additionally, 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.