TOWN OF GEORGETOWN, 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 Board of Selectmen
Town of Georgetown, Massachusetts

In planning and performing our audit of the financial statements of the Town of Georgetown, Massachusetts, as of and for the year ended June 30, 2018, in accordance with auditing standards generally accepted in the United States of America, we considered the Town of Georgetown, Massachusetts' internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Town's internal control. Accordingly, we do not express an opinion on the effectiveness of the Town's internal control.

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

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

Powers & Sullivan LLC

March 7, 2019

TOWN OF GEORGETOWN, MASSACHUSETTS

MANAGEMENT LETTER

JUNE 30, 2018

TABLE OF CONTENTS

PAGE

Current Year Comments

Framework for Assessing and Improving Cybersecurity

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 should an 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 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 take a pro-active approach and assess their 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.

The Town's insurance provider is currently providing some Cyber Liability Insurance coverage. We recommend that the Town assess the amount and type of liability coverage that best fits the Town's situation and consider continuing to carry insurance coverage 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.

Accounting for Fixed Assets

Comment

Since the implementation of GASB #34, the Town has compiled a detailed listing of all assets owned by the various departments of the Town. Maintaining this list requires the Town to account for additions, deletions, disposals and transfers of fixed assets. The Town has annually accounted for fixed asset additions; however, procedures have not been implemented for deletions, disposals or transfers. In order to maintain a complete and accurate fixed asset listing the Town needs to develop procedures to facilitate accurate fixed asset reporting.

Recommendation

We recommend that the Town develop and implement policies and procedures to ensure the proper accounting for all fixed assets by identifying and accounting for fixed asset deletions, disposals and transfers.

Prior Year Comments

Fixed Asset Capitalization Policy

Prior Comment

As part of the implementation of GASB #34, the Town had an initial accounting completed of all of their fixed assets. At that time, the Town established $5,000 as their threshold in determining which expenditures are capitalized and depreciated.

Based on the size of the Town's asset base and the types of assets being purchased and/or constructed, the Town should reevaluate the initial fixed asset policies adopted and consider the implementation of a higher dollar threshold for fixed asset capitalization. This would simplify the process by reducing the number of items that the Town capitalizes without significantly impacting the financial statements.

Current Status – *Resolved.* The Town voted to increase the capital asset threshold to $10,000.

Documentation of Internal Controls

Prior 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.

Current Status – *Unresolved*. There has been no change in the status of this comment.