TOWN OF GROVELAND, MASSACHUSETTS

MANAGEMENT LETTER

JUNE 30, 2019

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 Groveland, 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 Groveland, Massachusetts as of and for the year ended June 30, 2019, (except for the Groveland Municipal Light Department which is as of and for the year ending December 31, 2018) 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.

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 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 Groveland, 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

March 9, 2020

TOWN OF GROVELAND, MASSACHUSETTS

MANAGEMENT LETTER

JUNE 30, 2019

CONTENTS

Page

CONTINUING MATTERS PREVIOUSLY REPORTED

INVENTORY OF CEMETERY LOTS

Prior Comment

The Town does not currently have an adequate inventory control system to track the sale of cemetery lots and graves, nor does it have a comprehensive listing of the number of lots currently available. Additionally, during our audit we noted that the cemetery department does not have an adequate process to turn over the collection of funds relating to sales of lots and graves to the Town Treasurer in a timely manner.

Current Status

Resolved – The Town has organized the files and records in the cemetery office. The cemetery office is using its own database to track all lots and cemetery finances. All collections for the cemetery are taking place at Town Hall within the Treasurer's office.

FRAUD RISK ASSESSMENT

Prior Comment

The opportunity to commit and conceal fraud exists where there are assets susceptible to misappropriation and inadequate controls to prevent or detect the fraud. To address this risk, we recommend that the Town perform a risk assessment to identify, analyze, and manage the risk of asset misappropriation. Risk assessment, including fraud risk assessment, is one element of internal control. Thus, ideally, the Town's internal control should include performance of this assessment, even though our annual financial statement audits include consideration of fraud.

The fraud risk assessment can be informal sand performed by a management-level individual who has extensive knowledge of the Town that might be used in the assessment. Ordinarily, the management-level individual would conduct interviews or lead group discussions with personnel who have extensive knowledge of the Town, its environment, and its processes. The fraud risk assessment process should consider the Town's vulnerability to misappropriation of assets.

When conducting the self-assessment, questions such as the following can be considered:

- What individuals have the opportunity to misappropriate assets? These are individuals who have access to assets susceptible to theft and to records that can be falsified or manipulated to conceal the theft.

- Are there any known pressures that would motivate employees with the opportunity to misappropriate assets? Pressures may relate to financial stress or dissatisfaction. In assessing whether these pressures may exist, the assessor should consider whether there is any information that indicated potential financials stress or dissatisfaction of employees with access to assets susceptible to misappropriation.

- What assets of the Town are susceptible to misappropriation?

- Are there any know internal control weaknesses that would allow misappropriation of assets to occur and remain undetected?

- How could assets be stolen? Assets can be stolen in many ways besides merely removing them from the premises. For example, cash can be stolen by writing checks to fictitious employees or vendors and cashing them for personal use.

- How could potential misappropriation of assets be concealed? Because many frauds create accounting anomalies, the perpetrator must hide the fraud by running through an adjustment to another account. Generally, fraud perpetrators may use accounts that re not closely monitored.

Current Status

Unresolved - The Town has not yet developed or implemented a formal fraud risk assessment.

Continuing Recommendation

We continue to recommend that management develop and implement a fraud risk assessment program to identify, analyze, and manage the risk of asset misappropriation. Department heads should provide information detailing any activities within their departments that may lend themselves to potential fraud, i.e. identification of idle cash or collections that don't get turned over daily or instances where internal controls over Town assets are not in place or are not functioning as intended.

INTERNAL PROCEDURE MANUALS

Prior Comment

We noted that most departments do not maintain a formal internal procedure manual documenting day-to-day processing and controls. Since the Town is limited in the number of employees, the Town is at risk if critical tasks cannot be completed due to an extended absence.

Current Status

Unresolved - The Town has begun the process of identifying various departmental internal procedures in anticipation of completing the manuals, but this process is still in process as of the date of this report.

Continuing Recommendation

We recommend that an internal procedures manual be developed for each department. The document should be written in sufficient detail so that a person unfamiliar with the department's operations could complete the day-to-day critical tasks. Additionally, this document should be updated for any system changes. A master manual of all procedures should be maintained and stored in a secure, centralized location.

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 – The Town has not yet documented its internal control system over federal awards in compliance with the COSO Internal Control Framework.

Continuing 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.

Current Status

Partially Resolved – The Town is taking an active approach over cybersecurity. Within the past two years the Town has replaced their firewall. Additionally, the Town's insurance provider provides the Town with Cyber Liability Insurance coverage.

Recommendation

We recommend that management continue to 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.

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.