TOWN OF OAK BLUFFS, MASSACHUSETTS

MANAGEMENT LETTER

YEAR ENDED 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 Oak Bluffs, 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 Oak Bluffs, Massachusetts ("the Town") 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'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.

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.

Our consideration of internal control was for the limited purpose described in the first paragraph and would not necessarily identify all deficiencies in internal control that might be significant deficiencies or material weaknesses. We did not identify any deficiencies in internal control that we consider to be material weaknesses, as defined above.

However, we became aware of 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, 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 27, 2019

TOWN OF OAK BLUFFS, MASSACHUSETTS

MANAGEMENT LETTER

JUNE 30, 2018

TABLE OF CONTENTS

PAGE

PRIOR YEAR COMMENTS RESOLVED

In Fiscal Year 2018 the Town was able to address and rectify the matters noted below. Although these matters were not items that indicated major breakdown in internal controls, it appears that management treated these with the utmost importance.

LACK OF FORMAL POLICIES AND PROCEDURES MANUALS

Comment

There is a lack of formalized policies and procedures that documents the daily, monthly, and yearly procedures of staff members that are assigned to the Town's financial operations. While staff members account for finances under the Uniform Municipal Accounting System (UMAS) guidelines, UMAS does not get into the specifics as to how information should be accumulated from municipality to municipality. To date, the Town has begun to compile a master booklet of policies and procedures for all the key financial reporting offices; however, not all offices are fully documented and up to date in the specific detail of their operations.

Action Taken by Management to Resolve Matter

Management has been able to develop a comprehensive document that outlines various policies and procedures that touch upon the financial reporting process. This document sets polices for budget formation, capital needs and spending program, grants management, and cash reconciliations just to name a few of the items presented in the document. While this document is pending adoption by the Board of Selectmen, discussions with, and observations of management indicate that management is operating as if these policies are official.

USE OF PERSONAL CREDIT CARDS

Comment

Discussions with management indicate that certain departments encounter a recurring use of employees using personal credit cards for Town business. This appears to mainly be occurring in the EMS department when crews are off-island and encounter situations in which they need to pay for costs incurred while on Town business (i.e. ambulance break-down during transport to and from the island that require immediate mechanical attention and hotel stays due to missed boat connections). The Town currently does not have written policies that address the use of employee credit cards for costs incurred while performing an official Town function. The lack of written policies that address the use of personal credit cards for Town business is not sound business practice.

Action Taken by Management to Resolve Matter

The policy document, referred to in the first comment, has established acceptable and non-acceptable uses of Town issued credit/purchase cards. The document also puts in place policies to limit the Towns' exposure to potential fraudulent or abusive activity on the cards. Policies governing reimbursement rates, and limits on those reimbursement rates, for personal expenses incurred while conducting official Town business are also addressed.

FRAUD RISK ASSESSMENT

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 and 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 indicates potential financial stress or dissatisfaction of employees with access to assets susceptible to misappropriation.

- What assets of the Town are susceptible to misappropriation?

- Are there any known 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 are not closely monitored.

Action Taken by Management to Resolve Matter

Inside of the financial policies document discusses earlier, the Town presents an anti-fraud policy that:

- Establishes whistleblower protection;
- Establishes an overall framework that shares proper internal controls and fraud prevention among the department heads;
- Provides guidance to allow department heads to determine what may constitute an act of fraud;
- Establishes an investigative response to suspected instances of fraud;
- Provides tips to prevent Town related instances of fraud.

CONTROL OF MUNIS ACCESS AND USER RIGHTS

Comment

The process of allowing an employee to have access to MUNIS, and the process of assigning user rights to the employee's MUNIS profile, was not strictly governed and monitored. Currently, access to MUNIS is initiated by a phone call to the IT Director. The phone call could be initiated by a department head or a general employee but in almost all cases there is no document trail that would allow the IT Director to determine if the request for MUNIS access should be allowed or not. We have been told that sometimes "common sense" allows the Director to make a yes/no decision without having to consult with other members of Town management. On other occasions the IT Director will consult with, and defer to, the Town Accountant's advice regarding an access request.

Action Taken by Management to Resolve Matter

Management has implemented a policy in which the need to assign MUNIS user rights for new employees are determined during the time in which all new employees meet with Human Resources to undergo the typical new employee welcoming process. Once the personnel office determines such a need, a form requesting MUNIS access is forwarded to the accounting and IT offices for approval. Accounting and IT are also notified when employees are no longer employed by the Town so that applicable MUNIS user accounts can be deactivated.

TAILINGS

Comment

The Town has a current liability of approximately $20,000 that relates to checks that were written to vendors and/or employees, went unclaimed for a period, were voided and then record as a liability in accordance with the Commonwealth's abandoned property (tailings) laws. Since this liability has not been reconciled with the actual check listing of the Treasurer we can place no reliance on its accuracy.

We were able to review relevant documentation suggesting that the Treasurer is adhering to the abandoned property laws; however, we were not provided with a comprehensive document that details all the individual balances within the tailings account maintained by the Treasurer nor were we provided with documentation that would indicate that the Treasurer and Accounting Office is reconciling this account on a periodic basis.

Action Taken by Management to Resolve Matter

As of the end of fiscal year 2018 the ledger balance was unchanged from prior fiscal years; however, after June 30, 2018, the Treasurer's office was able to identify all checks that have been outstanding for 1 year or more. These checks have been voided with the bank and the appropriate entries have been posted to MUNIS to reflect the transaction.

ENTERPRISE FUND REPORTING

Comment

The Town presents a Wastewater Enterprise Fund in accordance with state law and generally accepted accounting principles (GAAP); however, the Town ledgers have not been appropriately adjusted to report these activities separately from governmental activities. As a result, management is faced with a process to extract

such information via spreadsheet and ledger reports to present the appropriate balances and activity for each fund.

The purpose of a computerized accounting system, such as the one employed by the Town, is to enhance transparency in the recording of transactions and to provide real time data that management can use to make time sensitive decisions in regard to funding and cash flow. Relying on a system that is dependent upon manual calculations increases the risk of error and slows down the timeliness of financial information produced.

Action Taken by Management to Resolve Matter

The Accounting Office recorded the appropriate accounting entries in MUNIS so that the general long-term associated with the enterprise fund is reported separately from non-enterprise fund debt. A series of MUNIS funds has also been reserved for specific use by future potential capital projects separately from governmental activities.

PRIOR YEAR COMMENT PARTIALLY RESOLVED

STUDENT ACTIVITY FUNDS

Comment

The Town maintains a combined student activity fund depository and checking account under the care, custody, and control of the school principal. The School is required to maintain its student activity funds, and related bank accounts, in a manner that is mandated by Massachusetts General Law, Chapter 71, Section 47. In reviewing the current procedures, we noted that enhancements are needed for the Town and School Department to comply with guidelines, issued by the Department of Elementary and Secondary Education, which provide suggested practices to assist towns and school districts in ensuring that the cash management of the student activity funds is managed according to MGL.

Massachusetts General Law Chapter 71 allows the school committee to authorize the Principal to receive money in connection with the conduct of certain student activities and to deposit such money, with the Town Treasurer into an interest-bearing bank account, established by the vote of the school committee to be used for the express purpose of conducting student activities. Interest earnings on such funds shall be retained by the fund and the school committee shall determine for what purpose such earnings may be used. In addition, the school committee needs to authorize the Town Treasurer to establish a checking account from which the funds may be expended exclusively for student activity purposes as authorized by the school committee. Funds received from student activities fundraisers and fees may only be deposited into an account under the care, custody and control of the Town Treasurer.

The school committee needs to vote and set the maximum balance that may be on deposit in the student activity checking account. The principal or designee, who operates and controls the student activity checking account, needs to be bonded in an amount determined by the Town Treasurer. To the extent that the funds are available in the student activity agency fund depository account, funds, up to the maximum balance set by the school committee, are to be transferred from the depository account through the warrant process to fund the related checking account. The process of replenishing the student activity fund checking account shall be subject to administrative procedures prescribed by the Town Treasurer.

Status

The school committee has established a $25,000 maximum that may be retained within the student activity fund checking account. Also, during 2017, School officials have obtained an appropriate level of bonding for school personnel who have care, custody and control of the checking account. No further activity occurred during 2018.

Continued Recommendation

We recommend that the Town establish the appropriate bank accounts as required under MGL. We also recommend that the Town and the School Department review the DESE guidance to ensure that all aspects of student activity fund cash management and operations are following MGL and DESE guidance.

As part of the Town's efforts to align fully with DESE guidance, we recommend that consideration be given to the audit requirements. The student activity funds should be audited internally on an annual basis and the audit needs to be documented in a manner suggested by DESE. Once every 3 years DESE indicates that the audit should be performed by an outside independent party.

UNRESOLVED COMMENTS OF THE PRIOR YEAR

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 are 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).

The COSO internal control framework is generally accepted as a best practice within the industry including the best practices prescribed by the Government Finance Officers Association (GFOA). COSO is a joint initiative of 5 private sector organizations dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence. The original COSO framework was published in 1992 and has been revised several times for changes in operations, technology, and audit risk. The most recent updates to the COSO Internal Control - Integrated Framework were issued in 2013 and are available at www.coso.org.

Management is responsible for internal control 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 incorporates 5 major components of internal control, which are supported by 17 principles of internal control as follows:

1. CONTROL ENVIRONMENT
    1) Demonstrates commitment to integrity and ethical values
    2) Exercises oversight responsibility
    3) Establishes structure, authority, and responsibility
    4) Demonstrates commitment to competence

5) Enforces accountability

2. RISK ASSESSMENT
   6) Specifies suitable objectives
   7) Identifies and analyzes risk
   8) Assesses fraud risk
   9) Identifies and analyzes significant change
3. CONTROL ACTIVITIES
   10) Selects and develops control activities
   11) Selects and develops general controls over technology
   12) Deploys through policies and procedures
4. INFORMATION & COMMUNICATION
   13) Uses relevant information
   14) Communicates internally
   15) Communicates externally
5. MONITORING
   16) Conducts ongoing and/or separate evaluations
   17) Evaluates and communicates deficiencies

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 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.

INFORMATIONAL COMMENT

FRAMEWORK FOR ASSESSING AND IMPROVING CYBER SECURITY

Comment

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. 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.

We also recommend that the community investigate 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.