Powers & Sullivan, LLC
CPAs AND ADVISORS

MASCONOMET REGIONAL SCHOOL DISTRICT

MANAGEMENT LETTER

JUNE 30, 2023

Powers & Sullivan, LLC
CPAs AND ADVISORS

100 Quannapowitt Parkway, Suite 101
Wakefield, Massachusetts 01880
T. 781.914.1700 | F. 781.914.1701
info@pas.cpa | www.pas.cpa

To the Honorable School Committee
Masconomet Regional School District

In planning and performing our audit of the basic financial statements of the Masconomet Regional School District (District) as of and for the year ended June 30, 2023, in accordance with auditing standards generally accepted in the United States of America, we considered the District's internal control over financial reporting 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 District's internal control. Accordingly, we do not express an opinion on the effectiveness of the District's internal control.

However, during our audit we became aware of matters that are an opportunity for strengthening internal controls and operating efficiency. The memorandum that accompanies this letter summarizes our comments and suggestions regarding these matters.

We will review the status of these comments during our next audit engagement. We have already discussed the comments and suggestions with District 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 District and is not intended to be and should not be used by anyone other than these specified parties.

Powers & Sullivan, LLC

March 27, 2024

MASCONOMET REGIONAL SCHOOL DISTRICT

MANAGEMENT LETTER

JUNE 30, 2023

TABLE OF CONTENTS

PAGE

Fraud Risk Assessment

Comment

The opportunity for errors or misappropriation of assets exists when there are inadequate controls to prevent or detect these types of transactions. To address this risk, we recommend that the District perform a risk assessment to identify, analyze, and manage the risk of asset misappropriation. Risk assessment is a key element of internal control that minimizes the possibility of misappropriation.

The risk assessment should be performed and documented in conjunction with management-level individuals who have extensive knowledge of the District that might be used in the assessment. Ordinarily, interviews and group discussions would be conducted with personnel who have extensive knowledge of the District, its environment, and its processes. The risk assessment process should consider the District's vulnerability to misappropriation of assets.

Recommendation

We recommend that management develop, document and implement a fraud risk assessment program to identify, analyze, and manage the risk of asset misappropriation.

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, 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 that may 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 the 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.