CliftonLarsonAllen LLP
CLAconnect.com

Management
Town of Groton, Connecticut

In planning and performing our audit of the financial statements of Town of Groton, Connecticut as of and for the year ended June 30, 2021, in accordance with auditing standards generally accepted in the United States of America, we considered the entity's 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 opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we do not express an opinion on the effectiveness of the entity's internal control.

However, during our audit we became aware of other matters that are opportunities to strengthen your internal control and improve the efficiency of your operations. Our comments and suggestions regarding those matters are summarized below. We previously provided a written communication dated February 18, 2022, on the entity's internal control. This letter does not affect our report on the financial statements dated February 18, 2022 nor our internal control communication dated February 18, 2022.

CURRENT YEAR RECOMMENDATIONS

Vendor Master File – Board of Education

During our audit we noted that no review of the vendor master file is occurring and access to this file is not limited. Access to master vendor files for purposes of adding new vendors or updating existing data should be extremely limited. Information entered into master vendor files should completed by one person and reviewed by a second. This limits the opportunity to set up a phantom vendor.

Recommendation – We recommend the Board of Education implement procedures to strengthen the controls around their vendor master file, including limiting the access to this file and segregating the duties of performance and review.

Cafeteria Bank Reconciliation – Board of Education

During the audit, we noted that the Board of Education had not fully reconciled the bank account balances for the Cafeteria fund with the general ledger until December of 2021. Due to the delays in reconciling cash in this fund, the year-end closing procedures were also delayed and the fund was not available to audit during the scheduled timeframe.

Recommendation – We recommend the Board of Education implement procedures to ensure that all bank accounts are reconciled to the general ledger on a monthly basis.

PRIOR YEAR RECOMMENDATIONS (REPEATED AND UPDATED)

Transfer Station Cash Collections

During the audit, it was noted that there is no formal collection process at the Transfer Station as there are multiple employees who have access to cash. There should be a process and associated documentation identifying who has the ability to collect cash/checks as well as who collected the cash. Once the cash is collected, the deposit should be reviewed by someone other than the employee who collected the cash.

Recommendation – We recommend the Town develop formal processes and controls over the cash collection and revenue recognition process which includes having the deposit reviewed by someone other than the employee who collected the cash. Additionally, we recommend the Town consider installing a camera to record the transactions and ensure that the collections are properly handled.

2021 Update – The Town is planning to install a CCTV camera in the shack to monitoring the cash box. The Town needs to install an underground conduit to run the CCTV wires. The Town anticipates having this done by March/April time frame.

Fraud Risk Assessment

According to the *2020 Report to the Nations on Occupational Fraud and Abuse by the Association of Certified Fraud Examiners*, 43% of corruption cases are detected by tip and half of the tips came from employees. In contrast, internal audit, the second most common detection method for corruption cases, uncovered 15% of these schemes. External audits and reports from law enforcement accounted for far fewer discoveries of corruptions, just 4% and 2%, respectively, of these schemes. Additionally, of the whistleblower tips that led to the investigation of the cases, 50% of those tips came from an employee and another 15% came from an anonymous source. Median losses were nearly doubled at organizations without hotlines.

During the annual audit, we do obtain an understanding of the Town's internal controls and assess the risk of fraud and whether or not the financial statements would be materially misstated due to these risks; however, an audit is designed to provide reasonable, but not absolute, assurance. Because of the inherent limitations of an audit, combined with the inherent limitations of internal control, and because we will not perform an examination of all transactions, there is a risk that material misstatements or noncompliance or fraud may exist and not be detected by us, even though the audit is properly planned and performed in accordance with auditing standards generally accepted in the United States of America. In addition, an audit is not designed to detect immaterial misstatements or violations of laws or governmental regulations that do not have a direct and material effect on the financial statements or major programs.

Recommendation – To address this risk, we recommend that the municipality 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.

The fraud risk assessment can be formal - performed by an outside accounting or consulting firm; or informal - performed by a management-level individual who has extensive knowledge of the Town that might be used in the assessment. The fraud risk assessment process should consider the Town's vulnerability to misappropriation of assets.

The fraud risk assessment should include a cybersecurity assessment. Cybersecurity is now considered a key business risk by most organizations. Being able to anticipate cybersecurity threats and develop strategies to prevent them is a critical part of a risk management program. Losses and recovery costs from data breaches, phishing attacks, ransomware and other incidents can be substantial. While the Town has implemented certain policies and procedures to reduce the risk of loss to a cybersecurity attack, a more formal approach to assessment and strategy is considered a best practice and should be considered.

An annual vulnerability assessment should be performed that identifies and evaluates exposures that could negatively impact the Town's ability to conduct business. This will identify your protected data, how it is stored, who has access and other critical information. It is then analyzed for security gaps based on your existing environment, and strategies are developed to mitigate those exposures. Successful strategies also include robust employee training, penetration and compliance testing, and protocols for responding to actual breaches, viruses and other attacks.

We will review the status of these comments during our next audit engagement. We have already discussed many of these comments and suggestions with various entity personnel, and we 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, the Town Council, and others within the entity, and is not intended to be, and should not be, used by anyone other than these specified parties.

CliftonLarsonAllen LLP

CliftonLarsonAllen LLP

West Hartford, Connecticut
February 18, 2022