blumshapiro
accounting • tax • advisory

29 South Main Street
P.O. Box 272000
West Hartford, CT 06127-2000
Tel 860.561.4000

blumshapiro.com

To the Members of the Board of Finance
City of Stamford, Connecticut

In planning and performing our audit of the financial statements of the City of Stamford, Connecticut, as of and for the year ended June 30, 2020, in accordance with auditing standards generally accepted in the United States of America, we considered the City of Stamford, Connecticut'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 City of Stamford, Connecticut's internal control. Accordingly, we do not express an opinion on the effectiveness of the City of Stamford, Connecticut's internal control.

We noted the following matters involving the internal control over financial reporting and its operation that we offer our recommendations as constructive suggestions for your consideration as part of the ongoing process of modifying and improving accounting controls and administrative practices.

The following matters involving internal control over financial reporting and its operation were noted in previous years but have not been fully remediated.

Schedule of Expenditures for State and Federal Single Audits

During the audit, we noted the completion of the state and federal schedule of expenditures was difficult to finalize. This was mainly attributable to delays in the completion of grant roll-forward schedules for both the operating and capital grants funds making it difficult to ensure the proper recording and testing of major programs for both the state and federal single audits. Although the process seems to be improving from year to year, we need the completion of the roll forwards to be timelier.

Recommendation

We recommend that the Grants Department, with the support of the relevant City departments and the Board of Education, complete its work in accordance with the timelines provided for in the instructions provided by the Controller's Office in its year-end closing memos using the reporting formats developed in conjunction with the Controller's Office so that the supporting documentation can be provided at the inception of our year-end audit field work. This will help ensure that the testing of major programs for the state and federal single audits can be completed in advance of the due dates for the state and federal single audit reports.

Internal Service Fund

The City is self-insured for police officers' and firefighters' heart and hypertension claims as required by state statute. The pay-as-you-go portion of the claims is paid from the City's Risk Management - Internal Service Fund. The City has committed surplus fund balance of $500,000 for FY2020 (proposed by administration and subject to approval by the Boards), $1,500,000 for FY2019, $250,000 for FY2018, $500,000 for FY2017 and $300,000 for FY2016. The City utilizes a third party to prepare an actuarial valuation to determine the heart and hypertension claims' liability. The claims' liability is being recorded at the government-wide level as required by GASB Statement No. 34, but it is not recorded in the Risk Management Fund.

Recommendation

We continue to recommend that the City record the heart and hypertension liability in the Risk Management Fund and establish a long-term plan to fund the deficit created by the recording of this liability.

GASB 87 - Implementation of Lease Standard – Postponed due to COVID-19

GASB No. 87, *Leases* is effective for fiscal years beginning July 1, 2021. It is critical that the City establish and execute an implementation plan that meets the reporting deadlines.

Recommendation

The City should inventory and review all current leases and contracts greater than twelve months to determine if they meet the GASB 87 definition of a lease. This will include all contracts where the City is the lessor or the lessee. The City should consider the following when establishing an implementation plan, including the purchase of any related software applications to support the financial reporting requirements required by GASB No. 87:

- Description of leasing arrangements
- Total amount of leased assets and accumulated depreciation by major class
- Commitments under leases before the commencement date
- Principal and interest requirements for the lease liability by fiscal year
- Tracking of any leasing transaction with related parties

Cybersecurity Management

Municipal governments must be proactive in securing operations and data. Cybersecurity strategies require new approaches to identify where critical information exists that needs to be protected, to foreseeing and deterring the threats that could result in the theft of information or the loss of funds, and to understand the overarching risks associated with cyberattacks. Proactively assessing and managing operations and IT environment(s) in anticipation of these threats and attacks is critical in light of the following:

- Nearly 70% of funds expended due to a cyber-event are unrecoverable and the scale of data breaches and lost funds due to phishing and business e-mail compromise is trending upward exponentially.
- Ransomware attacks force the majority of impacted government entities to pay to restore access to their data.
- Cybersecurity is now considered a key organizational risk, and spending on cybersecurity is projected to increase each of the next 10 years.

Recommendation

The City's TMS / IT department must continue its efforts to counter these on-going cyberthreats by:

- Following best practices in understanding the City's baseline exposure to cyberthreats through an annual security and vulnerability risk assessment to identify and evaluate exposures, hazards and/or potential for breach that could negatively impact the City's ability to conduct business.
- Using this assessment, identify and locate personal/confidential information (or other secure data) and understand how this information is currently secured to gain a clear understanding of the potential exposure.
- Risk mitigation plans can then be designed to tighten these areas of exposure and establish stronger security protocols. Resources should be applied to the areas most in need of protection and risk mitigation practices and procedures put into play.

A critical component of any organization-wide cybersecurity initiative is building and maintaining a resilient culture of cybersecurity by strengthening employee cybersecurity awareness through focused training. Assessing how employees respond to targeted threats through phishing simulation attacks can proactively identify areas of exposure, reinforce learning objectives, focus-in on training opportunities and help identify missing security protocols.

This letter should be read in conjunction with our report on Internal Control over Financial Reporting and on Compliance Based on an Audit of Financial Statements Performed in Accordance with *Government Auditing Standards* dated December 28, 2020.

This communication is intended solely for the information and use of management, Members of the Board of Finance, others within the organization, and federal and state awarding agencies and pass-through entities and is not intended to be and should not be used by anyone other than the specified parties.

Blum, Shapiro & Company, P.C.

West Hartford, Connecticut
December 28, 2020