KPMG LLP
Vaughan Metropolitan Centre
100 New Park Place, Suite 1400
Vaughan ON L4K 0J3
Canada
Tel 905-265-5900
Fax 905-265-6390

Mr. Stephen Conforti
Chief Financial Officer and Treasurer
City of Toronto
100 Queen St W,
Toronto, ON M5H 2N2

November 25, 2024

Dear Mr. Conforti,

In planning and performing our audit of the consolidated financial statements of The City of Toronto ("the Entity") for the period ended December 31, 2023, we obtained an understanding of internal control over financial reporting (ICFR) relevant to the Entity's preparation and fair presentation of the financial statements. This understanding was obtained to design audit procedures that are appropriate in the circumstances for the purpose of expressing an opinion on the financial statements, but not for the purpose of expressing an opinion on ICFR. Accordingly, we do not express an opinion on the effectiveness of the Entity's ICFR. We reported the results of our audit of the consolidated financial statements of the Entity to the Audit Committee on July 5, 2024.

Our understanding of ICFR was for the limited purpose described above and was not designed to identify all control deficiencies that might be significant deficiencies and therefore, there can be no assurance that all significant deficiencies or other control deficiencies have been identified. As a result, any matters reported below are limited to those deficiencies in ICFR that we identified during the audit. Our awareness of control deficiencies varies with each audit and is influenced by the nature, timing, and extent of audit procedures performed, as well as other factors.

Refer to the Appendix for the description of various control deficiencies.

Significant Deficiencies

As reported in our Audit Findings Report presented to the Audit Committee on July 5, 2024, we did not identify any control deficiencies that we determined to be significant deficiencies in ICFR.

Other control deficiencies

As we performed our audit, we identified control deficiencies that we determined to be other control deficiencies in ICFR that, in our professional judgment, are of sufficient importance to merit management's attention. See the Appendix for a listing of our audit observations relating to the control deficiencies that were identified from the audit of fiscal year ended December 31, 2023.

Management's responses

Management's responses have not been subjected to the audit procedures applied in the audit, and accordingly, we express no opinion on them.

Use of letter

This letter is issued annually (as applicable) for use by management in carrying out and discharging their responsibilities. This letter should not be used for any other purpose or by anyone other than management, auditor general and audit committee.

KPMG shall have no responsibility or liability for loss or damages or claims, if any, to or by any third party as this letter has not been prepared for, and is not intended for, and should not be used by, any third party or for any other purpose.

Yours very truly,

Licensed Public Accountants
cc: Auditor General

Appendix – Control Deficiencies from the audit of fiscal year ended December 31, 2023

The following control deficiencies are newly identified deficiencies by KPMG during the audit of fiscal year ended December 31, 2023 and were shared and discussed with management, during and subsequent to the 2023 audit.

1. Assets Under Constructions – Transfers

Observation:

During the audit, identified through testing the completeness of transfer of assets under constructions, multiples samples where the asset was substantially complete and had not been transferred in the current or prior periods. KPMG noted that these errors were in different divisions and communicated the absence of a formal annual assessment of assets under construction with indicators that there should be a transfer to completed assets to avoid these errors.

Impact:

Transferring assets under construction to completion late, incorrectly results in late recognition of amortization of the related cost over the useful life of the associated asset.

Recommendation:

It is recommended that the division responsible is provided training to ensure they understand the indicators that there should be a transfer to completed assets. Multiple WBS codes were identified as a potential reason that completed assets under constructions were not being transferred in the correct period. A formal policy detailing how WBS codes should be used to track a project and further oversight can help prevent these errors. In addition, divisions should provide timely updates about the project status to support the TCA reporting process.

Managements response:

As part of the City's ongoing work on the Financial Systems Transformation Program, the City will be developing a master data governance policy and related procedures for coding blocks, including WBS elements, to ensure that City divisions account for and report on their expenditures in a consistent manner by the City's estimated system go-live date of October 2025.

The City has also implemented other changes as part of fiscal 2024, such as the introduction of a mid-year project status validation process, as well as enhancement of existing training materials and resources to reinforce key accounting concepts, such as in-service date and asset transfers

Expected remediation date : October 2025

2. Asset retirement Obligation Testing – Source documentation

Observation:

During the recent audit, the audit team encountered challenges in obtaining original source documents. This issue was particularly acute in the Corporate Real Estate Management division, where documentation retention practices were inconsistent and management had difficulty providing backup to support asset attributes. As a result, the audit team had to rely on alternative sources to support the audit.

Impact:

The absence of readily available original source documents may results in an increase in inaccuracies in the financial and non-financial information for the City. This can further result in errors in financial reporting, operational inefficiencies, legal issues, and overall decision making by management and those charged with governance.

Recommendation:

To address the issues identified, it is recommended that the City implements a robust document retention policy that clearly defines the types of documents to be retained by each division depending on their area of focus. The City should ensure that this policy is communicated to all relevant employees and regularly reviewed for compliance. The City should conduct regular training sessions and awareness programs for employees, particularly in the real estate division, to emphasize the importance of proper documentation practices and adherence to the retention policy. The City should assign clear accountability for document retention and management to specific individuals or teams. The City should ensure that City employees understand their responsibilities and have the necessary resources to fulfill them effectively.

The Corporate Real Estate Management division is also recommended to preserve documentation related to the City's facilities and ensure that this information is accurately captured in the City's financial information system on a regular (e.g., annual) basis. Ideally, original documentation should be digitized and included in the Corporate Real Estate Management division's system to ensure that the information is accessible. By implementing these recommendations, the City can mitigate risks associated with document retention.

Management's response:

Management acknowledges the observation regarding the availability of source documentation across its Real Estate portfolio. Maintaining accurate and reliable source documentation to support the City’s real estate data is particularly challenging due to the age of many of its real estate assets, the variety of stakeholders and asset owners across the City, and the vast size and scale of the portfolio. The Corporate Real Estate Management division has already identified an initiative to validate and

refresh it's core real estate data, which will include, amongst other things, the following activities:

- Performing a review of existing real estate data against readily available source documents and identifying gaps or areas requiring verification.
- Revalidating existing building data through third party sources, where necessary, and updating the City's master real estate data which will be available to integrate with the City's financial information system, as needed.
- Reviewing existing processes, and developing / updating where necessary, to ensure source documentation is retained in accordance with the City's existing record retention schedule per Toronto Municipal Code, Chapter 217, Records, Corporate (City) and maintained in the City's real estate records.
- Documenting and communicating updated processes to all relevant staff and assigning clear responsibilities related to the ongoing management of the City's real estate data to ensure this data is accurate, reliable and retained in an accessible manner.

Expected remediation date : November 2025

3. Property and Liability Claims – Estimates

Observation:

It was noted that the data source and processes used by the City's actuary to determine the estimated property and liability claims has changed during the year and proper reconciliations were not completed by management. The changes in data source and aggregation created a disruption in the actuarial triangles from the case reserves front.

Impact:

Management needs to ensure that the "restated" historical triangles (historical claim data) are reliable foundations or there could be an issue with the data reliability and precision of the estimate completed by the actuary.

Recommendation:

We recommend that the Actuary or the City of Toronto should enhance the procedures about data sufficiency and reliability, such as:

- Reconcile the incremental paid and the case reserves with the carried amount in the financial statement,
- Compare historical triangles used in the current valuation with the ones in the previous valuation,
- Calculate the variations,
- Investigate the drivers for significant differences,
- Perform analysis sensitivities as necessary, and
- Document the procedures and conclusions in relation to the data sufficiency and reliability.

Management's response:

The City of Toronto and the City's Actuary have procedures in place to ensure data sufficiency and reliability as part of the actuarial process. The audit recommendations related to the City's Property and Liability Claims have been carried out and implemented, and results were presented to the auditor as part of their assessment.

Remediation date : November 2024

4. IT Security – Access Deprovisioning

Observation:

Access revocation tickets are not created by the Pension, Payroll, & Employee Benefits Division/ terminated user's manager from respective divisions in most cases, as a result; IT is not notified of the timely access revocations through the regular access revocation process. Access to systems was not always revoked in a timely manner. In certain instances, users logged into systems after their termination date.

Impact:

Failure to remove user access promptly after termination can result in unauthorized access to the City of Toronto's systems and financial information.

Recommendation:

Management should consider the following:

- To remediate this control deficiency, effective formal communication about the timeliness requirements in the access revocation process should be disseminated to all employees and managers across all divisions in the City of Toronto.
- Management should consider mandating the formal creation of tickets within the IT service management tool (ServiceNow) by the terminated employee's or contractor's manager. This will enable IT to revoke access from the Windows Active Directory in a timely manner.
- The City of Toronto should consider implementing a formal monitoring process over their automated workflow to revoke access from the SAP ECC application once a termination has been entered in the SAP SuccessFactors application. This will enable timely access revocation from the SAP ECC application.

Management's response:

A communication will be issued to all people leaders at the City of Toronto with respect to the importance of revoking employee access to City systems in a timely manner. Information was shared with people leaders through the corporate "Updates and Resources for Managers – October 20, 2024" newsletter.

In addition, the Manager and Supervisor Information Management Responsibilities Guidelines and Property Retrieval/Access Cancellation Checklist was uploaded to the People Leader Onboarding Program on ELI. This checklist includes guidance for people leaders in the technology access revocation process, including immediate suspension/cancellation procedures.

Effective October 16, 2024, the technology teams in the Pension Payroll & Employee Benefits & Technology Services divisions introduced a streamlined termination program within SAP-ECC. This program automatically revokes all SAP access and licenses for employees who have retired, resigned, or been involuntarily terminated. The action is triggered when an individual's termination is recorded in SuccessFactors.

Management also considering mandating the formal creation of tickets within the IT service management tool by Q4 2025.

Expected remediation date : Q4 2025

5. IT Security – User Access

Observation:

A complete user access review was not performed for the SAP ECC application. We also noted instances where the reviewers performed review of their own access. Additionally, the control does not operate at a sufficient precision to address the volume of employee turnover at City of Toronto because management performs the user access review only once a year.

Impact:

Users have access outside of which is necessary to carry out their job role and responsibility; and this may lead to excessive access.

Recommendation:

We recommend the following to TSD:

- TSD should modify its procedures to retain evidence of completeness and accuracy at the time of user access list extraction. This will boost the reliability of the user access review control process.
- The control performer should validate that all user access instances are sent to the respective role owners and managers for review. This will verify that all access instances are appropriately reviewed and authorized.
- The control performer should also promote proactive follow-ups to achieve timely completion of user access reviews. This will aid in maintaining the timeliness and effectiveness of the user access control process.
- TSD should put measures in place to prevent instances of self-review threats. In cases where such threats cannot be prevented, a secondary review from an appropriate reviewer should be mandated. This will uphold the integrity of the user access review process.

- TSD should consider conducting more frequent reviews, such as on a quarterly basis, to verify that all access is commensurate with job responsibilities. This will enhance the precision of the control activity to address the employee turn over at City of Toronto.

Management's response:

The City will address the recommendations through the following steps:

- Evidence of completeness and accuracy showing extraction criteria will be retained at the time of data extraction of user role assignments from system to evaluate completeness and accuracy of data extracted.
- Modified process to include raw data pivot tables to calculate row totals for each role owner against the total rows of user role assignments from system to ensure completeness of user role assignments sent for review.
- Modified the process to include verification of the spreadsheets that role owners submit once review is completed to ensure all user role assignments are appropriately reviewed and authorized.
- Updated process for review of role owner's user role assignments by their respective managers to address self-review threat.
- The periodic user-role-access verification will continue to be performed annually.

Remediation date : May 2024

6. IT Security – Segregation of duties in change management

Observation:

Segregation of duties between development and deployment of the changes to production environment are not enforced as part of the logical access design. Further, it was observed that multiple changes in the transport log from SAP ECC were developed and deployed by the same user.

Impact:

Lack of segregation of duties between change development and deployment enable a developer to circumvent the change management process which may result in unauthorized or unapproved changes to systems or programs that may affect system and data reliance and functionality.

Recommendation:

City of Toronto should design and implement appropriate segregation of duties between change development and deployment functions within the SAP ECC application. If the implementation of the recommended segregation of duties is deemed unfeasible by management, we suggest that they should strengthen monitoring controls. Specifically, the reviewer should be tasked with verifying whether changes deployed to the

production environment are authorized and adhere to the established change management process.

Management's response:

The City will address the requirement for segregation of duties in change management in the SAP ECC application through the following steps:

- Where feasible, management will either downgrade the permissions on accounts by removing deployment access or converting to non-interactive system accounts to address segregation of duties conflict in system.
- The import process was modified in the fall of 2023 to include a check to avoid having the SAP & Technical Solution Services team accidentally promote their own transport(s).
- SAP Release Compliance Management team has implemented a semi-annual process to review transports that have moved to Production to check for any breaches of Segregation of Duties. In cases where the developer and importer are the same user, there will be follow up to ensure an appropriate rationale.

Expected remediation date :Q4 2024

7. IT Security – Super User Access

Observation:

Multiple accounts had inappropriate access to SAP ECC system's sensitive transaction codes which are considered to provide a user with privileged access. Further, it was noted that password for some generic accounts was shared amongst multiple users which are not subject to monitoring.

Impact:

Granting access to sensitive transaction codes on SAP ECC application can potentially give a user excessive access and create more segregation of duty conflicts than necessary for their job role. Additionally, allowing multiple users to access generic accounts without implementing a fire call process or regular monitoring activities could potentially result in inappropriate/unauthorized activities without a user being held accountable.

Recommendation:

TSD should consider the following recommendations to address the risk:

- Frequently reviewing user access, such as every quarter, to sensitive transaction codes can help to identify and rectify any inappropriate access. This should be done on a periodic basis and any changes should be documented and approved by management.
- Where possible, passwords for generic accounts should not be shared amongst

multiple users. Instead, each user should have their own unique password. This can help to ensure that each user is held accountable for their actions.

- Where management doesn't deem it feasible to restrict access to an account to only one user then they should consider implementing a fire call process (such as firefighter process or password vaulting process). A fire call process can help to ensure that access to generic accounts is only granted on an as-needed basis and is closely monitored. This can help to reduce the risk of inappropriate/unauthorized activities.
- Where management doesn't deem it feasible to restrict access to an account to only one user then they should consider implementing regular monitoring activities. Regular monitoring activities can help to identify any inappropriate/unauthorized activities. This should include monitoring of user activity, system logs, and access controls.

Management's response:

The City will address the requirement for sensitive access on SAP ECC application through the following steps:

- Annual user access review has been enhanced to highlight access to sensitive roles with sign off from role owners.
- Introducing a periodic monitoring process for the identified generic accounts with sensitive access to ensure activities performed by users were authorized.

Expected remediation date : Q4 2024

8. IT Security – Incident Resolution

Observation:

Management did not continue monitoring open incidents on a periodic basis upon implementing ServiceNow tool in FY 2023, which replaced HPSM tool. Some incidents were not resolved in a timely manner, per service level agreement (SLA). As a result, there is delay in incident resolution for five (5) of 25 selected service requests where the incident resolution delay is between 1 and 3 days.

Impact:

Unresolved incidents or incidents which are not resolved in a timely manner may lead to inaccurate or incomplete processing of data on production systems.

Recommendation:

TSD should consider implementing the monitoring process for open/long outstanding incidents on a periodic basis like how it was performed when HPSM tool was used. This will help management analyse, investigate, and resolve SLA breaches and understand the root-cause in effort to alleviate repeated incidents.

Management's response:

The City will address the requirement for incident resolution process in the ServiceNow tool through the following steps:

It is important to note that given the diversity of incidents and applications, targets at the ServiceNow level are not policies, but general guidelines (per document "IT Incident Management Reference Guide" referenced by this audit).

Upon review, this document was found to contain inconsistencies (e.g. "SLA" acronym being used without "guideline" descriptor in 4 locations, and timings not consistently articulated as "Business Days").

With that context, the following step will be taken:

- The guideline document noted above will be updated to resolve these inconsistencies.

In terms of the ticket status, currently ServiceNow platform:

- Sends automated emails to ticket assignee and their manager when ServiceNow level guideline SLA is being breached
- Enables fulfilling teams to build personalized Dashboards/reports to monitor their queues.

In order to remove the barrier of dashboard/report creation, and to provide a standardized view on ticket status:

- A standardized ServiceNow Incident Dashboard will be developed to be leveraged by the teams

Expected remediation date : Q1 2025

9. IT Support – ServiceNow SOC Report

Observation:

Management did not retain evidence of ServiceNow's SOC report review.

Note: ServiceNow is Software as a Service ("SaaS") based IT service management tool which enables key internal controls over financial reporting (ICFR) such as access provisioning, access deprovisioning, change management and incident management.

Impact:

Lack of SOC report review may lead to lack of vendor risk management over the ServiceNow vendor controls which may potentially impact ICFR controls at City of Toronto.

Recommendation:

TSD should implement a process to review the SOC report and retain the evidence of their review. While this is not an all-inclusive list, the review should reflect management's assessment over audit opinion expressed by the service auditor in the SOC \report, audit period covered, bridge letter considerations, risk assessment of the exceptions noted in the SOC report, mapping of management's controls against the relevant complementary user entity controls (CUEC) with gap assessment on unmapped CUECs, and subservice organization carveout considerations.

Management's response:

All reviews of SOC report 1 & 2 were completed via security assessment required for deployment, but evidence was not retained. We will ensure moving forward that appropriate evidence is recorded. Going forward, process will be stood up to review SOC report 1 and flag any new risk and remediation.

Expected remediation date : Q1 2025