Report
Audit Committee
The Corporation of the City of Brampton
November 24, 2020

IMPROVEMENT REQUIRED

Date: September 22, 2020

Subject: **Segregation of Duties**

Contact: Sunny Kalkat, Director, Internal Audit, 905 874 2215,
satinder.kalkat@brampton.ca

Executive Summary:

Internal audit completed an independent review of Segregation of Duties (SoD) operating and application controls to ensure that incompatible functions are properly segregated and that access is granted on a minimum use basis.

The concept of SoD is to separate the major responsibilities of authorizing, custody, recording and verification of transactions and assets. No one employee should have responsibility to complete two or more of these major responsibilities. SoD is applied between single individuals (individual-level SoD) and between functions or organizational units (unit-level SoD). SoD is further managed through application controls.

The systems included in the assessment were: PeopleSoft Financials, PeopleSoft Human Capital Management (HCM), AssetWorks M5 for fleet asset management, and, Hansen for linear asset management.

The background, scope and objective are explained in **Appendix 1**.

Our review identified the following strengths in the processes:

Unit-Level SoD	Reviewed the separation of incompatible functions at the business unit level, for example accounts payable and purchasing. No issues noted.
Individual-Level SoD	Reviewed the separation of incompatible job functions and supporting application access controls. For example authorized users may create purchase requisitions, but purchase orders are created by authorized purchasing roles. No issues noted.

IT Development and Production SoD	Reviewed the separation of incompatible IT developer roles and IT production support roles. No issues noted.
IT Support Roles SoD	Reviewed the separation of incompatible IT system administrator (SA) roles and database administrator (DBA) roles. No issues noted.
IT DBA SoD	Reviewed the separation of DBA development and production support roles. SoD is not in place due to the size of the team however, appropriate compensating controls are in place.
Transactional SoD	Reviewed accounts payable transactions, payroll adjustments and employee record changes to ensure they were performed by authorized personnel. No issues noted.

An updated employee onboarding process has been implemented. The implementation of an updated off-boarding process is on hold due to COVID-19.

Special Note

The employees suspended in April 2020 as a COVID-19 cost cutting measure were allowed to retain access to the City's network and electronic mail. This was done out of respect for the employees with the view that the employees are still members of the organization who will be returning to work as soon as possible. This resulted in higher instances of unauthorized accounts, and we have adjusted our counts accordingly.

Internal Audit discussed the following improvement opportunities with Digital Innovation and Information Technology:

Process	Finding	Rating
User Access and Identity Management	Employees suspended in April on temporary basis retained their access to sub-systems in addition to network and email access.	P3

These issues and associated management action plans are explained in more detail in **Appendix 1.** These issues are rated as per criteria explained in **Appendix 2.**

Conclusion:

Improvement is required to ensure that access to information systems and applications are removed upon termination of employment or reviewed upon change of employment within the City. Improvement is also required to user access management reviews of the operational asset management systems.

In Opportunities for Improvement, **Appendix 1**, deactivating obsolete roles and associated user accounts would create efficiencies with fewer user accounts and roles to manage, and further decrease the risk of misuse. Standardizing system user naming conventions and security practices in application development road maps would set development towards consistent application security management.

We have rated inherent risk as high due to complexity of our operations and the dollar value of assets under management by various departments.

Overall report rating is determined as criteria for audit report rating explained in **Appendix 3**.

We thank all participants for their support and efforts during the audit.

Authored by:

_____

Richard Gervais, Sr. Advisor, IT Audit
Internal Audit

Reviewed and Approved by:

_____

Sunny Kalkat, Director
Internal Audit

Submitted by:

_____

David Barrick
Chief Administrative Officer

Appendices:

Appendix 1: Segregation of Duties
Appendix 2: Criteria for Audit Report Rating
Appendix 3: Criteria for Evaluating Audit Findings

Segregation of Duties – Audit Report

Audit Name	Segregation of Duties (SoD)		
Sponsor(s)	Chief Information Officer, Digital Innovation and IT, Corporate Services		
Business Unit	Digital Innovation and IT, Human Resources, Finance, Public Works, Transit, Community Services	**Date Issued**	September 22, 2020

1.0 Executive Summary

Audit Rating and Conclusion

Overall findings
Improvement is required to ensure that access to information systems and information processing facilities are removed upon termination of employment or reviewed upon change of employment. Improvement is also required to user access management reviews of the operational asset management systems.

The inherent risk was evaluated as high due to the complexity of our operations and the dollar value of assets under management by various departments.

During our review, some of the strengths we found in the processes are as follows:

- SoD are in place at the organizational level and supporting applications. For example, the tasks of creating purchase requisitions, generating purchase orders, and accounts payable are segregated between the operating departments, Purchasing and Finance, respectively. Similarly, Human Resources maintain employee records but payroll is managed in Finance.
- SoD are in place at the individual level. Role-based access control is in place at the individual level.
- User access management reviews are in place for the financial and human resources management systems.
- Digital Innovation and IT (DIIT) and Human Resources (HR) have implemented an on-boarding process. The completion of the off-boarding process is delayed due to COVID-19.

Internal Audit discussed the following improvement opportunities with Digital Innovation and Information Technology:

- Standardized system user naming conventions and security practices must be included in application development roadmaps.

- Deactivation of obsolete roles and associated users would decrease the risk of misuse. Reducing the number of roles and active accounts will also enhance the user access review.
- There are only three database administrators, and we acknowledge that segregation of development and production database administrator roles is not practical. We are satisfied with the compensating controls are in place, including:
    - Database logs are aggregated by a contracted third party, who monitors the database logs and notifies CoB IT security of any changes or suspicious activity,
    - Database administrators logon to systems using named user accounts,
    - Database changes are all subject to the change management process and management oversight,
    - There is segregation between system administrators, developers and database administrators roles, and,
    - Third-party database access is supervised by the CoB database administrators when it is needed, and third-party access is revoked after completion of the work.

These issues and associated management action plans are explained in more detail within the body of this report. Other less significant items, as well as more details related to observed issues, were also provided and discussed with management involved in the related activities.

Appendix 1

Background, Objectives, and Scope

Our audit objective was to independently review segregation of duties (SoD) operating and application controls to ensure that incompatible functions are properly segregated, and that access is granted on a minimum use basis.

In general, the principal incompatible duties to be segregated are:

- Custody of assets,
- Authorization or approval of related transactions affecting those assets,
- Recording or reporting of related transactions, and,
- Verification or control duty.

During the review, we utilized data analytics to understand and assess user access information as well as financial information.

The period under review was June 1, 2019, to May 31, 2020.

The scope of our review included:

- Review SoD policies, procedures and application controls.
- Interviews with key personnel.
- Review of controls intended to prevent and detect:
    - Non-compliance with the policies and procedures, and,
    - Processing of unauthorized transactions.
- Adequacy and effectiveness of related management oversight in case incompatible functions are improperly segregated.
- Change management of SoD roles and assignment.

Appendix 1

2.0 Detailed Audit Findings and Proposed Management Actions

Rec #	Audit Findings	Finding Rating	Proposed Management Action	Responsible Party	Completion Date
1	Employees suspended in April on a temporary basis still retained their access to sub-systems in addition to only network and email.	P3	Management will assess appropriate contingency plans that will prevent or monitor for inappropriate access through the period of the suspension.	Manager Client Services, HR. Manager Client Services, IT.	September 30, 2020

3.0 Other Opportunities for Improvement (Minor issues)

Rec #	Audit Comments
1	**Obsolete roles** There are still active roles in place in the financial system that are no longer needed due to the fact that the business functionality has been moved to sub-systems. We noted over 350 user accounts could be deactivated in the PeopleSoft Financials. For example, the P-Card functionality has been moved from PeopleSoft to the BMO platform. The majority of these users no longer need to be active in PeopleSoft.
2	**Standardizing system user naming conventions and security practices** Assessing user-access across multiple systems highlighted challenges to enterprise-level user account management. We observed the following: • Naming conventions vary from system to system, and more so in older systems. • Existing system capability to automate user access management reporting varies from system to system. Older systems were not designed to support this approach.

Appendix 1

Rec #	Audit Comments
	• A user access report provided for the chosen systems was not readily available for M5. This may create a barrier to implementing automated and efficient user access management reviews. Management should consider integrating standardized user naming conventions and standardize security administration practices in each system's development map.

Appendix 2 – Criteria for Evaluating Audit Findings	
Priority Rating	**Description**
Priority 1 (P1)	**One or more of the following conditions exist that require immediate attention of the Senior Leadership Team. Corrective actions by senior management must be implemented.** • Financial impact of both actual and potential losses is material • Management's actions, or lack thereof, have resulted in the compromise of a key process or control, which requires immediate significant efforts and/or resources (including time, financial commitments, etc.) to mitigate associated risks. Failure by management to remedy such deficiencies on a timely basis will result in the City being exposed to immediate risk and/or financial loss • One more of the following conditions is true: i) management failed to identify key risks, ii) management failed to implement process and controls to mitigate key risks • Management's actions, or lack thereof, have resulted in a key initiative to be significantly impacted or delayed, and the financial support for such initiative will likely be compromised • Management failed to implement effective control environment or provide adequate oversight, resulting in a negative pervasive impact on the City or potential fraudulent acts by City staff • Fraud by management or staff, as defined by the Corporate Fraud Prevention Policy (Policy 2.14)

Priority 2 (P2)	**One or more of the following conditions exist that require attention by senior management. Corrective actions by management should be implemented.** • Financial impact of both actual and potential losses is significant • Management's actions, or lack thereof, may result in a key process or control to be compromised, which requires considerable efforts and/or resources (including time, financial commitments etc.) to mitigate associated risks • Management correctly identified key risks and have implemented processes and controls to mitigate such risks, however, one or more of the following is true: i) the processes and controls are not appropriate or adequate in design, ii) the processes and controls are not operating effectively on a consistent basis • Management's actions, or lack thereof, have impacted or delayed a key initiative, and the funding for such initiative may be compromised • Management failed to provide effective control environment or oversight on a consistent basis, resulting in a negative impact on the respective division, or other departments • Management failed to comply with Council-approved policies, by-laws, regulatory requirements, etc., which may result in penalties • Management failed to identify or remedy key control deficiencies that may impact the effectiveness of anti-fraud programs
(Priority 3) P3	**One or more of the following conditions exist that require attention by management. Corrective actions by management should be implemented.** • Financial impact of both actual and potential losses is insignificant • A non-key process or control, if compromised, may require some efforts and/or resources (including time, financial commitments, etc.) to mitigate associated risks • Processes and controls to mitigate risks are in place; however, opportunities exist to further enhance the effectiveness or efficiency of such processes and controls. Management oversight exists to ensure key processes and controls are operating effectively • Minimal risk of non-compliance to Council-approved policies, by-laws, regulatory requirements, etc. • Low impact to the City's strategic or key initiative • Low impact to the City's operations

Segregation of Duties – Audit Report
Private & Confidential
Appendix 3: Criteria for Audit Report Rating

Rating	Description
Effective	• Key controls are adequately and appropriately designed, and are operating effectively to support objectives and manage risks • Audit recommendations resulted in only minor enhancements to the effectiveness or efficiency of controls and processes • One or more Priority 3 Findings • Insignificant cumulative financial impact when all audit findings have been considered • Audit findings would not be subject to a follow-up by Internal Audit
Improvement Required	• A few control weaknesses were noted that require enhancements to better support objectives and manage risks • One Priority 2 and Priority 3 findings • Priority 3 findings only where the cumulative financial impact is significant • Corrective action and oversight by management is needed • Audit findings could be subject to a follow-up by Internal Audit
Significant Improvement Required	• Numerous key control weaknesses were noted that require significant improvement to support objectives and manage risks • One Priority 1 finding or more than one Priority 2 findings and Priority 3 findings • Priority 2 and 3 findings only where the cumulative financial impact is significant • Corrective action and oversight by senior management is required • Audit findings will be subject to a follow-up by Internal Audit
Immediate Action Required	• Key controls ae either not adequately or appropriately designed and are not operating effectively, or there is an absence of appropriate key controls to support objectives and manage risks • More than one Priority 1 finding, combined with Priority 2 or 3 findings • Regardless of the type of findings, the cumulative financial impact is material to the City's financial statements. • Confirmed fraud by management or staff • Corrective action and oversight by Senior Leadership Team is required immediately • Follow-up of such audit findings by Internal Audit would be of high priority