Information Technology Projects Implementation:

Information Privacy and Cybersecurity Review of Human Resource System

February 3, 2021

Beverly Romeo-Beehler, FCPA, FCMA, CFF, ICD.D, JD, B.B.A.
Auditor General

AUDITOR GENERAL TORONTO

Table of Contents

Executive Summary

The City implemented a new human resource system in 2019

The City of Toronto implemented a new human resource (HR) system in 2019 to replace its old HR modules in human resource management and administration. This new integrated HR system provides an end-to-end workflow, from recruitment to hiring and onboarding for new staff. It collects and stores a significant amount of information relating to individuals, including elected officials. Because of this, it is extremely important that this system has strong measures addressing cybersecurity and information privacy in place.

Auditor General became aware of a data incident through the Fraud Hotline

In early 2020, the Auditor General became aware of an issue concerning access to system data through a Fraud Hotline complaint. Given the importance of information privacy and cybersecurity, the Auditor General immediately initiated a review of the system implementation process, in the context of overall information security at the City.

Cybersecurity and information privacy have always been high-priority areas for the Auditor General

Cybersecurity and information privacy have always been high-priority areas for the Auditor General. Since 2015, the Auditor General has performed a number of audits of the City's IT infrastructure and critical systems (Refer to Appendix 2) and has recommended controls to improve cybersecurity and information privacy. The Auditor General will continue to perform audits and assess evolving cybersecurity and information privacy risks.[1]

Objective to assess information privacy and security controls

The objective of this review was to assess the implementation of information privacy and cybersecurity controls of this new HR system, and to recommend measures to address any weaknesses identified during the review.

Findings evaluated in the context of City-wide processes

While this review focused on the implementation of the HR system, we also considered City-wide processes and believe that the findings may be systemic. As a result, many of the recommendations are applicable to other ongoing and future technology implementations, such as the current category management solution (ARIBA) and Salesforce.

[1] The City hired a Chief Information Security Officer in October 2019 after this project was underway. He was not involved until after the incident that was the subject of the complaint. Still, the lessons learned will help further protect security going forward.

More detailed and technical report has been provided to management

To maintain confidentiality, we have not provided specific details of the incident in this public report. However, the recommendations made in this report provide a high-level view of the controls that must be strengthened. A second, more technically detailed report has been provided to management.

This is a review not an audit

This is a review of allegations concerning operational issues with respect to cybersecurity and information privacy. The procedures and work performed in this report do not constitute an audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). However, we believe the work performed and information gathered provide a reasonable basis for our findings, conclusions and recommendations.

Summary of Findings

Staff were mistakenly assigned higher-than-required privileged access and three incidents occurred

The first incident occurred in late 2019 when a group of staff were mistakenly assigned higher-than-required privileged access roles during the initial system implementation. This resulted in the group of staff potentially having the capability to access information that was not required for purposes of their work responsibilities. Furthermore, the implementation was rushed so the configuration was not tested completely in the production environment before the system was launched.

Remediation actions from the first incident were not implemented quickly enough

Two further instances of inappropriate access occurred because the recommendations to remedy the first incident were not fully implemented quickly enough. The inappropriate access provides capability to access certain information that may not be needed as part of work responsibilities.

The following are areas that must be addressed in order to strengthen the security and privacy of information when implementing technology projects at the City:

A. Project governance must be strengthened

Strengthen project governance

Project governance processes must be strengthened at the City in relation to how it manages major technology implementations. Our review identified the City needs to:

Implement 'privacy by design' principles

1. Implement 'privacy by design' principles as an essential component for all technology projects. A privacy review of the design choices of various user roles was not performed to ensure role designs met best practices.

Improve communication and transparency

2. Improve communication and transparency between project team members and stakeholders. Key stakeholders should be involved from the early phases of the project and fully understand all the risks involved, take accountability on reviewing and accept the risks that exist in each project phase.

Timely and proactive management of cybersecurity and privacy risks

3. Evaluate and manage cybersecurity and information privacy risks in a timely manner. Gaps, when identified, should be communicated and addressed before the system is moved into production. In this case, the privacy assessments were not updated, and the City Clerk's Office ant the People & Equity Division were not advised of the risks with the new roles and system changes implemented before the system "went live" in September 2019.

Implement remediation actions identified in the incident response report in a timely manner

4. Address and manage all incidents in a timely manner. The remediation actions identified in the initial response report issued in February 2020 were still outstanding at the time of this review in July 2020. This led to further incidents being reported.

5. Clearly document the process for addressing cybersecurity and information privacy incidents for consistent implementation across the City.

Ensure compliance with project management approval processes

6. Ensure compliance with project management approval processes. Document approval decisions prior to moving to the next phase of the project. For example, we were advised that the system was being moved to production on the verbal approvals by the stakeholders. Informal or undocumented approvals demonstrate weak project governance.

Review user roles with specific focus on financial transactions processing

7. Implement review of financial controls. The system is heavily related to financial matters and the adequacy of internal controls is extremely important. The user roles' capabilities and features were not reviewed with a specific focus on financial transactions processing.

Improve access controls and activity logging

B. User access controls and activity logging needs improvement

Management needs to:

Large number of users with Super Administrator privileges create security risks

1. Limit the use of Super Administrator access. Super Administrator access has unique entitlements which can result in elevated risks. Excessive use of these Super Administrator access accounts increases cybersecurity and information privacy risks.

In addition, as this role can create records, edit details and view all data in the system, it could also compromise financial controls.

2. Strengthen user logging and monitoring activities. Limitations of user logging capabilities are a security control risk.

Limited user logging capabilities are a security control risk

The City needs to strengthen controls to monitor access logs of Super Administrator accounts and also the anonymous accounts used by the vendor. The anonymous accounts were set-up by the vendor to be shared among the support staff.

Support and sustainment staff roles need to be developed

3. Define clear roles and responsibilities for post implementation support and sustainment staff. The City should change the current practice of assigning Super Administrator roles to support staff; instead develop specific roles that align with the requirements of support staff.

System testing needs to comply with IT standards

C. System testing needs to comply with IT standards

The City needs to improve system testing. The system testing did not fully comply with the standards outlined in the project's master test plan. Complete end-to-end business process testing was not conducted prior to implementation, and concerns raised were not fully addressed and communicated to stakeholders. Post-implementation validation (PIV) has not been fully performed.

Recommendations will help the City better manage technology project implementations

The Auditor General has made 10 recommendations. The recommendations contained in this report guide the City in taking appropriate and immediate actions to address the issues identified, reduce the exposure of private information and increase system security. They will also help the City to better define the processes it needs to manage technology project implementations and to monitor and respond to cybersecurity and information privacy incidents in a timely manner.

We express our appreciation for the co-operation and assistance we received from management and staff of the Technology Services Division, City Clerk's Office, Pension Payroll & Employee Benefits Division and People & Equity Division. The timely provision of information and coordination of various activities greatly assisted in completing this review and report in a short amount of time. We would also like to acknowledge management and staff from the Office of the Chief Information Security Officer.

Management Comments

Management advised that the Office of the CISO and the City Clerk have been engaged to ensure that the changes being deployed as part of the stabilization of this system are reviewed and monitored, and that risks to cybersecurity and information privacy are not elevated.

In addition, management is working to finalize a standard response process for potential cybersecurity and information privacy incidents, and also coordinating with the vendor to improve auditing and reporting capabilities. The management actions will be verified during our follow-up of recommendations made in this report.

Detailed management comments and action plan for each of the recommendation is provided in Appendix 1.

Background

Implementation of integrated human resource management solution began in 2017

The City initiated the implementation of an integrated human resource management solution in 2017. The objective of this implementation was to merge existing HR functions, from vendor provided and in-house systems, into one system. These functions include management of organizational structures, jobs, positions, employee master data and enabling enterprise-wide workflows.

HR system collects and stores personally identifiable information

The HR system has several modules that collect and store significant information relating to users, such as employees and elected officials. This information is needed in order to manage employee records, recruitment and payroll. The System currently has over 40,000 users.

Key Stakeholders

Implementation of HR management system involves all City divisions

The implementation of this HR management system involved all City divisions, and each division is a stakeholder as it uses this system to manage staff recruitment and other HR matters. However, certain divisions have a greater role to play and we have described those divisions as key stakeholders.

TSD is responsible for implementing and coordinating this system across the City

The Technology Services Division (TSD) is responsible for both implementing the system and coordinating it across the City. Other key stakeholders are:

The Clerk is the City's records custodian

- The City Clerk's Office: The Clerk is a mandatory statutory officer appointed by City Council under the *City of Toronto Act, 2006 (COTA)*. In addition to fulfilling legislative requirements under COTA, and as the head designated by City Council for purposes of *Municipal Freedom of Information and Protection of Privacy* Act (MFIPPA), the City Clerk leads the Office of the City Clerk and ensures that all statutory obligations are administered to fully comply with legislated record retention requirements. As such, the Clerk is the City record custodian and must be fully engaged with privacy, information and record management system decisions.

People & Equity Division manages the City's human resources

- People and Equity Division (P&E): This Division is entrusted with the management of the City's human resources, equity and human rights functions.

PPEB Division manages City payroll and maintains employee information

- Pension, Payroll and Employee Benefits Division (PPEB): This Division administers the City's employee pension plans and benefit packages. It also processes the City payroll and maintains employee information.

All City staff and elected officials have a profile in the HR system

All City staff and elected officials have their profile set up in the system. These profiles include information relating to the individuals (hereafter referred to as "Personally Identifiable Information" or "PII"), such as name, date of birth, contact information, position, salary, emergency contact etc. Employees can use the self-service functionality in this system to update the information contained in the assigned profile entries.

The Auditor General received complaint via the Fraud Hotline about inappropriate access

Complaint to the Auditor General

In early 2020, the Auditor General became aware, through a Fraud and Waste Hotline complaint, of concerns that the new HR system implementation led to inappropriate levels of access being assigned to individuals and that risks may continue to exist. The complaint stated that inappropriate access privileges were provided to a large number of staff. As a result, information of City staff and elected officials became potentially accessible to those who did not require access for purposes of work responsibilities.

The City took immediate action, correcting any known incidences of access privilege levels being assigned inappropriately and issued a communication about the incident to all affected staff and elected officials.

Given the importance of information privacy and cybersecurity during the COVID-19 pandemic the Auditor General proceeded with the review with the assistance of Technology Services Division, the City Clerk's Office, P&E and PPEB staff, and the Office of the CISO. A detailed technical report was provided to the Technology Services Division, Office of the CISO, City Clerk's Office, P&E Division and PPEB Division.

Review Results

A. Project Governance must be strengthened

Good project governance is critical for the successful completion of a project. It provides accountability, direction and defines decision-making procedures. It also provides criteria for validating impacts to the project and enables issue resolution to occur in a timely manner.

Trying to execute a large IT project with an inadequate governance structure results in a lack of control over project deliverables and stakeholders' management. Good project governance needs to be clearly defined at the initial design phase and should address how decisions and accountabilities are disseminated and assigned between the project team, executives and stakeholders.

Without a concrete governance structure, project stakeholders were not able to provide input on important project components such as:

- Privacy Impact Assessment (PIA)
- Threat Risk Assessment (TRA)
- User Acceptance Testing (UAT)

The following sections provide details of findings and recommendations.

A. 1. Privacy risks are not fully evaluated from inception to post-implementation

Cybersecurity and information privacy risks should be considered from inception to post-implementation

A successful project implementation includes a well-defined and thought-through process during the planning stage, considering all potential risks to information privacy and cybersecurity from inception to post-implementation.

'Privacy by Design (PbD)' is an approach for developing new technologies and systems. According to a former Ontario Information Privacy Commissioner, Ann Cavoukian, PhD[2],

> *"The Privacy by Design (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after."*

[2] https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf

Privacy by Design principles were not incorporated in the project implementation

We found that '*Privacy by Design'* principles or equivalent steps were not incorporated as a guiding roadmap in the project implementation and not all key stakeholders were fully aware of the potentially relevant concerns regarding information privacy and cybersecurity. The City Clerk's Office, for example, became involved in May 2019, two years after the project was initiated. Thus, they did not have an opportunity to provide input into the design of the project's roles and accountabilities.

Privacy assessments are performed to ensure an organization complies with:

- Privacy requirements set out in MFIPPA[3], and
- Other relevant legislative requirements

PIA was conducted two years after project initiated

A Privacy Impact Assessment (PIA) was conducted by the City in April 2019, which was almost two years after the project began. The PIA should have been completed in the early stages of the project to ensure the right risks were considered, the right stakeholders were engaged and proper governance was in place to address any issues.

Privacy review of user roles design not performed

After April 2019, the project underwent many design and configuration changes, including changes to user roles and privileged accounts. A review of the design and configuration changes was not performed to ensure the previous PIA remained an accurate review of the project in light of the changes to role designs and configuration.

Assessment of cybersecurity and information privacy concerns should be continuous

An assessment of these potential concerns should be a continuous process and must be considered with the original design of the system, as well as when changes are made. The Information and Privacy Commissioner of Ontario guidance on conducting PIA's [4] states:

> *"…as project implementation progresses, continue to assess the project's privacy risks and impact to determine if you need to update your privacy analysis and PIA report.*
>
> *This ongoing assessment is an essential part of identifying and mitigating new issues and changes impacting privacy that arise during implementation."*

[3] https://www.ontario.ca/document/freedom-information-and-privacy-manual/introduction-act#:~:text=1%20MFIPPA%20The%20Freedom%20of,institutions%20covered%20by%20the%20Acts.
[4] https://www.ipc.on.ca/wp-content/uploads/2015/05/planning-for-success-pia-guide.pdf

A. 2. Risks identified in TRA were not properly communicated and addressed

Threat Risk Assessment (TRA) identifies security risks

In addition to the PIA, a Threat Risk Assessment (TRA) was performed during 2019. A TRA identifies cybersecurity and information risks and provides an opportunity for IT to evaluate security controls and assist management in making decisions on risks.

Risks identified in TRA not mitigated prior to system launch

We noted that there were 15 risks (11 medium and 4 low risks) identified. These risks were not mitigated prior to the system being launched in September 2019.

Not all stakeholders fully understood and formally accepted the risks

The project team accepted the level of risks identified in the TRA. Based on our discussions and review of documents, we found that not all stakeholders may have fully understood and formally accepted the risks. Some of the key stakeholders were not consulted at all, such as the City Clerk, so input was not received from them on the TRA.

Uninformed decision-making could lead stakeholders accepting elevated risks

There is a need to improve communication, transparency and understanding around information privacy and cybersecurity risks with key stakeholders. This process should also be formalized. Communication is one of the essential elements of good governance and is a contributing factor of a project's success or failure. It is necessary that all stakeholders, and in particular the key stakeholders, are involved in the project from inception to completion. Uninformed decision-making can potentially lead stakeholders to accept elevated risks.

A. 3. Information privacy and Cyber Security incidents are not managed in a timely manner and consistently documented

Information privacy and cybersecurity risks not managed in a timely and proactive manner

Our review found that the City did not manage the information privacy and cybersecurity risks concerning this system in a timely and proactive manner both before and after the launch of this system.

First incident September 2019

The project team and the City Clerk's Office investigated the first access incident that occurred in September 2019. They developed a report about the root cause of the error, and outlined the actions required to fix the problem.

Ten months to plan for remedial actions from first incident

However, it was not until 10 months later that the proposed improvements stemming from that incident were scheduled to be completed (between September and December 2020). Management advised that the COVID-19 pandemic is among the reasons for the delayed action. The information privacy and cybersecurity risks continued to exist by the time we completed our review in October 2020.

Further incident February 2020

Meanwhile, another incident occurred in February 2020, where it was again noticed that some staff in a Division had been granted access rights which may not be limited to access to only information specifically required for purposes of work responsibilities. A review of this incident found that had they addressed the recommendations from the September 2019 incident, it may have prevented this and a subsequent incident.

Ten-month delay in developing of a plan for remediation not good incident management practice

A 10-month delay from the time of the first incident to the definition of a remediation plan does not reflect good incident management practices. The cybersecurity best practices, such as, NIST[5] and ISO[6] guidelines require a comprehensive plan to be in place to analyze and respond to security incidents in a timely manner. Taking more time at the start of a project helps to prevent cybersecurity and information privacy incidents.

It is important for the technology implementation teams to understand the City's information management obligations, and to act upon the recommendations in a timely manner.

Documentation of Security Incidents

Practices need to be documented, communicated and implemented

The City has practices in place to handle cybersecurity and information privacy incidents. For example, certain forms need to be completed when a security or privacy incident occurs, and meetings to review the incident are to be held in order to identify issues and take corrective actions. These practices need to be formally documented, communicated and implemented City-wide, including the City agencies and corporations.

All incidents not consistently documented and followed-up

Our review indicates that not all of the incidents discussed in this report were documented and consistently followed-up. In the context of the overall IT environment at the City - which is comprised of over 50 Divisions, complex IT infrastructure and a large number of applications - there is a need to centralize the management of cybersecurity and privacy risks in a unit or designated staff to ensure incidents are consistently documented and addressed in a timely manner.

In June 2019, the Auditor General tabled a supplementary report at Audit Committee entitled "Establishment of City-wide Cybersecurity Breach Incident Management Procedures Required[7]". In this report, the Auditor General recommended the following:

[5] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
[6] https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:ed-1:v1:en (not all information is publicly available)
[7] https://www.toronto.ca/legdocs/mmis/2019/au/bgrd/backgroundfile-135368.pdf

"City Council request the City Manager, the Chief Information Officer and the City Clerk to coordinate and develop standard incident management procedures, including communication protocols to address incidents involving cyber attacks/information breaches. The procedures and protocols should include:

a) Guidelines describing the sequence of actions that should take place as soon as staff become aware of a cyber attack/information breach incident
b) Communication protocols detailing key contact names, functions and contact information for staff to receive guidance
c) Reports to be completed by the affected organization, detailing the date of incident, systems affected, information compromised, and other relevant details
d) Communications to the media/public, where required, including privacy protocols.

The incident management procedures and communication protocols should be liaised across the City, including agencies and corporations."

Inconsistencies in addressing incidents could have negative impact

Without following a documented incident response process for identifying, assessing and remediating root causes of cybersecurity and information privacy incidents, we expect there will be inconsistencies in addressing security or privacy incidents across the City. This could have a negative impact on implementing remedial actions in a timely manner to address the risk of reoccurrences and unaddressed risks.

Recommendations:

1. **City Council request the Chief Technology Officer enhance the management of cybersecurity and privacy risks as part of its IT project governance by:**

    a. **Ensuring that cybersecurity and information privacy requirements and related budget are part of the acquisition, development and design phases of technology projects. The Office of the Chief Information Security Officer and the City Clerk should be consulted to review the budget allocated for cybersecurity and information privacy for all City technology initiatives, transformations and procurements.**

b. Ensuring a process is in place to identify, analyze and communicate all cybersecurity and information privacy risks to all stakeholders at each project phase through a documented risk mitigation plan. The identified risks are either mitigated or formally accepted by the division head/ project sponsor before the system is launched.
c. Ensuring the remediation of open risks is completed within a specified timeline and are signed off by the division head/ project sponsor before moving to next project development stage.

These actions should be extended to existing in-progress technology projects and all future implementations.

2. City Council request the Chief Technology Officer enhance the City's incident response process by:

a. Ensuring all incidents are logged in a consistent manner and addressed and communicated to the appropriate stakeholders in a timely manner.
b. Actively monitoring remediation actions and ensuring that processes are in place to test the post-remediation environment.
c. Coordinating with the City Clerk to integrate the privacy incident response process with the Office of the CISO's Cyber incident response plan and Technology Service Division's Major Incident Management process.

These actions should be considered in addition to the Auditor General's previous recommendation included in the report entitled "Establishment of City-wide Cybersecurity Breach Incident Management Procedures Required"

A. 4. Project management phases not managed properly

The Project Management Office uses methodology comprised of five major phases, referred as "Gates"

The Technology Services Division Project Management Office uses project management methodology that is comprised of five major phases, referred as "Gates". Table 1 provides brief descriptions of these gates. Gate review is performed by the project review team at the end of each phase to determine if required tasks in each gate are complete.

A Go/No-Go decision is made after the review and approval of the stakeholders. The project then proceeds to the next phase or 'Gate'.

Table 1: Technology Services Project Phases (Gating Criteria)

Project Phase	Gate	Description
Concept	Gate 1	Review Concept Summary that will outline the problem or opportunity and indicate how it is strategically aligned with the corporate objectives.
Definition	Gate 2	The Concept is elaborated on to articulate what the future state would look like and describes what process changes would be required. The outline of the scope in the Business Case is expanded further by the Project Manager in the Project Charter and the project schedule is created.
Planning	Gate 3	Ensure that all aspects of the project are identified, planned and appropriately documented. Key activities include capturing the business requirements and affirming the scope of the project in detail.
Implementation	Gate 4	This is the last gate before implementation and rollout of the project, representing the final point at which the project review team along-with all the stakeholders can review project activities have been completed before it is put to productive use.
Close-Out	Gate 5	Complete all outstanding project activities and verify all deliverables are complete and signed, lessons learned, and benefits captured.

Could not conclude whether all key stakeholders were included in the design, build and testing phase of the project

The project team advised that the project passed gate reviews for gates 1, 2 and 3. However, the project did not successfully pass-through gate 4. Some deficiencies identified in Gate 4 were not corrected and remained outstanding. We received insufficient support to conclude whether all key stakeholders were included in the design, build and testing phase of the project[8].

Gate 4 is a very important gate (final gate) before the project is implemented. This gate represents the last point at which the stakeholders can review project activities and determine completion before it is launched to the production environment. At this point, the users will start using the system and entering data into it

Outstanding risks not mitigated but project moved ahead anyway

Based on our discussions with the project manager and key stakeholders, and review of documents, we noted that some outstanding risks were not fully mitigated. The Project Management Office made the decision to move the system to production, despite the identified gaps, due to the tight delivery timelines of the project.

Verbal approvals to move to production

No meeting minutes were provided to document participants, decisions and actions from the meeting. We were advised that a verbal approval was provided by stakeholders during the night the system was being moved to production.

[8] We requested to review the Gate 1, 2 and 3 approvals. We were advised that while approvals were obtained, they could not be located.

Recommendations:

3. **City Council request the Chief Technology Officer to enhance project governance by:**

   a. **Ensuring all projects fully comply with the Project Review Team gating approvals. Exceptions relating to cybersecurity and privacy should be reviewed by the Chief Information Security Officer, and the City Clerk for a Go/No-go decision.**
   b. **Ensuring project management gating criteria include a clear support transition plan when projects move from development to operations or from one stage to the next, depending on which project management methodology is used, such as Agile project management[9].**
   c. **Ensuring project managers are trained in change management methodology.**

4. **City Council request the Chief Technology Officer in coordination with the Chief Information Security Officer and the City Clerk develop a training program for project managers and key staff involved in the implementation of technology initiatives to receive cybersecurity and information privacy training focused on managing technology projects.**

   In addition, the Chief Information Officer conduct an assessment to determine the feasibility of extending this training program to major agencies and corporations.

A. 5. Roles and responsibilities not clearly defined

Roles and responsibilities should be clear

According to the Project Management Institute (PMI) best practice, effective project management requires that project requirements, scope, roles and accountabilities be clearly documented and stabilized at some point early in the project life cycle. This includes the role of the project manager, project team members and key stakeholders.

For example, the project began in the spring of 2017, but key stakeholders, including the City Clerk's Office and PPEB Division, were not included until a much later stage. The City Clerk's Office, for example, was involved two years after the project start, in May 2019, thus they did not have opportunity to provide input into the design of the project roles and accountabilities.

[9] Agile project management is composed of several iterations or incremental steps towards the completion of a project (https://www.pmi.org/learning/library/agile-project-management-pmbok-waterfall-7042)

The privacy resource was not in place for the duration of the project, and sustainment support roles were not clearly defined. Without clearly defined roles in the project planning stage, it was difficult to determine who was the right person or group to accept the risks and sign off at each gate.

Recommendation:

5. City Council request the Chief Technology Officer to enhance the project governance and project management framework by ensuring:

a. All stakeholders' roles and responsibilities are clearly defined and key stakeholders are involved from the project initiation stage.
b. A clear support transition plan when project is moved from development to operations at Gate 4, the last gate before the system is moved to operations.
c. The City Clerk and the Chief Information Security Officer are part of the project steering committee for all key technology initiatives and transformations that involve privacy and security risks.
d. Criteria are developed to determine projects with high risks that have not been mitigated prior to moving to production be escalated to the Senior Leadership Team (SLT). The developed criteria should be shared with the City Manager for city-wide implementation.

A. 6. Lack of adequate review of internal controls

Review of the system design not performed with specific focus on the internal controls

We noted that although the system is heavily related to financial matters and the adequacy of internal controls is extremely important, no review of the system design was undertaken with specific focus on internal controls. The roles, capabilities, and features were not reviewed for segregation of duties in relation to financial transaction processing.

The use of the Super Administrator role in some operational areas could also represent a lack of segregation of duties. For example, while using Super Administrator access, a user can create records, and change information that could be used to process unauthorized transactions.

Recommendation:

6. **City Council request the Chief Technology Officer to enhance project management framework by including a review of internal controls for systems that involve financial transactions. The Controller's Office or Internal Audit should be involved in the review of user roles in relation to financial transaction processing to ensure appropriate segregation of duties is maintained for all user roles.**

B. User Access Controls and Activity Logging Needs Improvement

B. 1. Large number of Super Administrator and anonymous accounts present security risks

Roles are designed for specific needs

The system has specific roles which are designed for various users to perform their work responsibilities. It is important that these roles are designed with due care, thoroughly tested and assigned to staff according to business needs. While there are many roles have been created in the system, we are describing three roles in the context of our review:

Three roles examined

1. A 'Super Administrator' role is the highest possible privileged role available in the system and supersedes all user access roles. Since it has such capabilities, the use of this account should be tracked and restricted. The vendor's recommended guidelines indicate that only one person per organization (with one or two backups for redundancy) should have the Super Administrator role.

2. A 'Division Administrator' role allows the user to access all system functionalities, including access to employee records and the capability to make changes in the system for that division.

3. A 'Basic Employee' access role will provide a "view" access only to the employee's own records.

In July 2020, there were 90 users who had Super Administrator access

When we began our review in July 2020, there were 90 users who had Super Administrator access. These accounts were later reduced to 53. We noted 12 of these 53 accounts were anonymous accounts. The anonymous accounts were created for support roles and were used by multiple staff of the vendor.

Multiple Super Administrator accounts are a risk to information security and privacy

Having a large number of Super Administrator accounts is a high risk to information security and privacy. This risk is further elevated when anonymous users have Super Administrator access.

The following quote from CSE[10] (Communications Security Establishment) underlines the importance of the Principle of Least Privilege:

"Minimizing the number of users with domain or local administrative privileges is mitigation measure #4 on the CSEC Top 35 Mitigation Measures list. The concept of Least Privilege is designed to enhance security by reducing user access privileges to the minimum required to perform job related tasks."

"Problems arise when privileged users consistently access the system using their privileged access rights, such as:

- *While working, a legitimate privileged user may make a mistake and inadvertently cause damage to the network environment; and/or*
- *An intruder may gain access to a legitimate privileged-users' credentials which gives them unfettered access to valuable information assets and the opportunity to deliberately modify systems that the privileged-users control."*

The issues of excessive super administrative roles and the use of anonymous/generic user accounts have been reported in many previous audit reports by the Auditor General. These accounts are a potential risk and could become a source of data compromise.

B. 2. Need for detailed access logging reports

Detailed activities performed or information accessed by the user are not always logged/tracked

Data access logs are used to monitor for unauthorized access of data, and act as evidence or provide a trail of activity in order to investigate data breaches. This feature helps to ensure all users and administrative staff are following internal guidelines, and helps prevent and track security incidents.

Logging of user activities should be strengthened, in particular for users with elevated access roles, for example, a user with Super Administrator or Division Administrator access role.

Use of anonymous users with Super Administrator access must be stopped, except where approved as an exception by senior management.

[10] https://cyber.gc.ca/en/guidance/cyber-journal-edition-3-summer-2013

No review of logging functionality

There are 42 unique roles created in the System. These roles provide various levels of access and capabilities to users. A detailed review should be conducted to determine that logging functionality is appropriate to suitably address the cybersecurity and information privacy concerns with respect to the 42 unique user access roles. The lack of such a review indicates that there are potential risks to the confidentiality of information.

Recommendations:

7. **City Council request the Chief Technology Officer improve the user permissions framework of the Human Resources application. This includes:**

    a. **Conducting the cybersecurity and information privacy review of the various roles created in the HR system.**
    b. **Reviewing the users with a Super Administrator role and limiting the number of users with that role considering the industry's best practices and professional bodies.**
    c. **Ensuring that user access roles are designed with cybersecurity and information privacy in mind. The access roles should be provided to users on a 'need to have' basis.**
    d. **Defining a process for the approval of access roles for support staff. Instead of providing Super Administrator access, the support staff should be provided access on a 'need to have' basis.**
    e. **Eliminating the use of generic and anonymous accounts. If these roles are needed as an exception for operational reasons, detailed monitoring and logging procedures should be developed and implemented for these roles.**

    In addition, the review of elevated access roles, use of generic or anonymous users should be extended to the SAP enterprise application.

8. **City Council request the Chief Technology Officer to develop standards and minimum criteria for logging user activity details for IT systems. Steps include but are not limited to:**

    a. **Ensuring user access logs capture account activity for users with elevated access, such as, users with Super Administrator or Divisional Administrator roles.**
    b. **Implementing a user activity review process for roles with elevated access on a periodic basis to ensure access is aligned with the role.**

C. System Testing Needs to Comply with IT Standards

C. 1. User acceptance testing (UAT) "conditionally" approved

Comprehensive user testing of the HR system was not completed

A comprehensive and full user testing of the HR system was not completed. User Acceptance Testing (UAT) is the last test cycle of the project implementation and is an essential part of gaining end user acceptance. According to the Vendor's System Testing Guidelines, *User Acceptance Testing (UAT):*

> *"... should test the complete, end-to-end business processes to verify that the implemented solution performs the intended functions and satisfies the business requirements."*

A complete end-to-end business process test must be completed for all projects. Key stakeholders who are responsible for the information in the system, such as the City Clerk's Office should be involved in the user acceptance testing. All testing should be completed by respective stakeholders and approved accordingly. We found some user acceptance testing was conditionally approved.

Incomplete test cycles or non-compliance with exit criteria may lead to an increased risk of critical defects after a system goes live.

C. 2. Post-Implementation Validation testing (PIV) not performed

Post-Implementation Validation (PIV) is a phase of testing that verifies that whether the manually transferred system configuration (set-up) in the production environment is accurate and conforms to the system tested and approved in the testing environment.

The PIV is important in particular for systems that do not use automated tools for moving them from test environment to production. The HR system was manually transferred to the production environment.

Post implementation validation was not completed

Our review indicates that complete PIV testing was not completed for this HR system. As a result, errors in configuration of user access roles were not identified and resulted in inappropriate access being provided to a number of users.

A quality assurance or post-implementation review for manual configuration changes could have assisted in identifying the errors in configuration.

Recommendations:

9. City Council request the Chief Technology Officer to implement a process to ensure comprehensive system testing and user acceptance testing is part of the overall IT project management methodology. This includes:

    a. Assigning staff having subject matter expertise in Technology Services Division or Office of the Chief Information Security Officer to review the test scope, test cases and test cycle defect management.
    b. Ensuring that user acceptance testing is started early in the project stage and performed by respective divisions (users). In situations where, testing is performed by staff other than the User Division, the test results must be formally approved by the respective Division Lead contact on the project.
    c. Ensuring each test cycle go through a formal approval process and mandatory security testing prior to commencing the next test cycle.

10. City Council request the Chief Technology Officer to research options to automate the move of configuration of systems from testing to the production environment.

    Alternatively, include a peer review (Quality Assurance) to verify post implementation configuration in the system after it has been moved to the production environment.

Conclusion

Enhanced project governance needed

The Auditor General concluded that enhanced project governance is needed. The key stakeholders' involvement in the design, knowledge transfer and testing of the system is extremely important to ensure cybersecurity and information privacy requirements are met before the system launch.

Need to focus on identification and management of risks

The project should continue to focus on identification and management of cybersecurity and information privacy risks, and the timely implementation of remediation actions to mitigate the risks to an acceptable level.

Communication to stakeholders will help management

Increased transparency and proactively communicating risks to all relevant stakeholders (business data owners, data custodians, compliance, security and privacy) will help management make informed decisions on cybersecurity and information privacy requirements, devise mitigation strategies and identify testing needs prior to a project's implementation.

Ten recommendations to address cybersecurity and information privacy issues

The Auditor General has made 10 recommendations. This review will assist the City in implementing corrective measures to address the findings and ensure processes are in place to monitor and respond to cybersecurity and information privacy issues and incidents (if any) in a timely manner and also assist in implementing controls for other technology implementations.

A technical report has been provided to management in November, 2020 in order to correct critical issues immediately.

Objectives, Scope and Methodology

Objective:

The objective of this review was to evaluate the privacy and security controls of the recently implemented HR System; the incident response practices that were set in place to respond to the cybersecurity and information privacy incidents and the project management processes to identify and prevent further risks.

Scope and Methodology:

The scope of work included:

- Understanding the IT environment and controls by reviewing relevant documents, policies and procedures and meeting with staff to enquire, and document understanding of the project and processes
- Interviewing the business and IT stakeholders on IT processes
- Completing a high-level review of the HR system security controls currently implemented in the system (user access, activity logging and monitoring, configuration, security and privacy incident logging and reporting, ongoing monitoring and response processes in place
- Reviewing implemented mitigation actions and controls prior to deployment and post deployment of the system
- Performing various types of tests, such as, segregation of duties, analyse results, identify false positives, where needed in coordination with project team members and respective division staff
- Documenting issues relating to configuration, conflicting roles, inappropriate access etc. and provide recommendations to address them

The team performed the review considering the best practices published by the Office of the Privacy Commissioner of Canada (OPC) guidance on performing Privacy Impact Assessments (PIAs) for new or redesigned programs, cybersecurity good practices and Treasury Board Secretariat Directive for segregation of duties.

The procedures and work performed in this report does not constitute an audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). However, we believe the work performed and information gathered provide a reasonable basis for our findings, conclusions and recommendations.

Appendix 1: Management's Response to the Auditor General's Report Entitled: "Information Technology Projects Implementation: Information Privacy and Cybersecurity Review of Human Resource System"

Recommendation 1: City Council request the Chief Technology Officer, enhance the management of cybersecurity and privacy risks as part of its IT project governance by:

a. Ensuring that cybersecurity and information privacy requirements and related budget are part of the acquisition, development and design phases of technology projects. The Office of the Chief Information Security Officer and the City Clerk should be consulted to review the budget allocated for cybersecurity and information privacy for all City technology initiatives, transformations and procurements.
b. Ensuring a process is in place to identify, analyze and communicate all cybersecurity and information privacy risks to all stakeholders at each project phase through a documented risk mitigation plan. The identified risks are either mitigated or formally accepted by the division head/project sponsor before the system is launched.
c. Ensuring the remediation of open risks is completed within a specified timeline and are signed off by the division head/project sponsor before moving to next project development stage.

These actions should be extended to existing in-progress technology projects and all future implementations.

Management Response: ☒ Agree ☐ Disagree

Comments/Action Plan/Time Frame:

The Chief Technology Officer will enhance the management of cybersecurity and privacy risks as part of its IT project governance by:

a. Reviewing and updating project governance to ensure that the business case for business and technology projects includes cybersecurity and information privacy requirements and related budget. The appropriate consultation with the Office of the Chief Information Security Officer and the City Clerk will be done through project governance – **Q3 2021**
b. An updated project governance will be established to ensure that cybersecurity and information privacy risks are proactively identified, documented and communicated to all relevant stakeholders at each project phase through a Risk Mitigation Plan. The identified risks will be either mitigated or formally accepted during project reviews and meetings, by the Division Head/Project Sponsors before the system is launched – **Q3 2021**
c. Regular project governance will ensure that specified timelines are followed for remediation of open risks in the Risk Mitigation Plan and that risks are either mitigated or formally accepted by the Division Head/Project Sponsors as part of defined Exit Criteria before moving to the next project development stage – **Q3 2021**

Expected implementation date: **Q3 2021**

Recommendation 2: City Council request the Chief Technology Officer, enhance the City's incident response process by:

a. Ensuring all incidents are logged in a consistent manner and addressed and communicated to the appropriate stakeholders in a timely manner.
b. Actively monitoring remediation actions and that processes are in place to test the post-remediation environment.
c. Coordinating with the City Clerk to integrate the privacy incident response process with the Office of the CISO's Cyber incident response plan and Technology Service Division's Major Incident Management process.

These actions should be considered in addition to the Auditor General's previous recommendation included in the report entitled "Establishment of City-wide Cybersecurity Breach Incident Management Procedures Required".

Management Response: ☒ Agree ☐ Disagree

Comments/Action Plan/Time Frame:

TSD has an Enterprise IT Service Management (ITSM) Process that follows the IT Infrastructure Library (ITIL) v3 framework. This process includes incident and problem management resolution activities that includes cyber-related incidents. The processes were built in collaboration with the Office of the CISO. This process includes a detailed incident response process that is governed by a Security Operations Centre that is chaired by the office of the CISO. To further enhance the process, CTO will ensure:

a. Mandatory compliance of critical systems with the ITSM process including (not limited to) incident logging, stakeholder communication, tracking remediation actions, testing post-remediation environment, The City Clerk's privacy incident response plan will be integrated with the Office of the CISO's Cyber incident response plan and Technology Services Division's Major Incident Management process.
b. Please refer to response: a.
c. Please refer to response: a.

Expected implementation date: Draft available in Q3 2021

Recommendation 3: City Council request the Chief Technology Officer to enhance project governance by:

a. Ensuring all projects fully comply with the Project Review Team gating approvals. Exceptions relating to cybersecurity and privacy should be reviewed by the Chief Information Security Officer, and the City Clerk for a Go/No-go decision.
b. Ensuring project management gating criteria include a clear support transition plan when projects move from development to operations or from one stage to the next,

depending on which project management methodology is used, such as Agile project management[11].

c. Ensuring project managers are trained in change management methodology.

Management Response: ☒ Agree ☐ Disagree

Comments/Action Plan/Time Frame:

The Chief Technology Officer will enhance project governance by:

a. Establishing an updated Project Review process with appropriate Gating Model. Project Review Team will ensure mandatory compliance with the Gating Model for all capitally funded projects that meet the established criteria. The PRT gating model to include review and sign-off of exceptions relating to cybersecurity and privacy by the Chief Information Security Officer and the City Clerk for a Go/No-go decision. – **Q3 2021**
b. Ensuring the PRT Gating Model includes a support transition plan from 'project' to 'operations' for all projects at last gate before moving to production stage or from one stage to another, depending on which project management methodology is used, such as Agile project management – **Q3 2021**
c. Conducting assessment of the change management needs to prepare Change Management training. All Project Managers will be trained in change management methodology – **Q4 2021**

Expected implementation date: **Q4 2021**

Recommendation 4: City Council request the Chief Technology Officer in coordination with the Chief Information Security Officer and the City Clerk develop a training program for project managers and key staff involved in the implementation of technology initiatives to receive cybersecurity and information privacy training focused on managing technology projects.

In addition, the Chief Information Officer conduct an assessment to determine the feasibility of extending this training program to major agencies and corporations.

Management Response: ☒ Agree ☐ Disagree

Comments/Action Plan/Time Frame:

The Chief Technology Officer will coordinate with the Chief Information Security Officer for cybersecurity training material and with the City Clerk for information privacy training material to educate project managers and key staff involved in the implementation of technology initiatives– **Q4 2022**

[11] Agile project management is composed of several iterations or incremental steps towards the completion of a project (https://www.pmi.org/learning/library/agile-project-management-pmbok-waterfall-7042)

Expected implementation date for City Divisions and an agreed approach for major agencies and corporations: **Q4 2022**

Recommendation 5: City Council request the Chief Technology Officer to enhance the project governance and project management framework by ensuring:

a. All stakeholders' roles and responsibilities are clearly defined and key stakeholders are involved from the project initiation stage.
b. A clear support transition plan when project is moved from development to operations at Gate 4, the last gate before the system is moved to operations.
c. The City Clerk and the Chief Information Security Officer are part of the project steering committee for all key technology initiatives and transformations that involve privacy and security risks.
d. Criteria are developed to determine projects with high risks that have not been mitigated prior to moving to production be escalated to the Senior Leadership Team (SLT). The developed criteria should be shared with the City Manager for city-wide implementation.

Management Response: ☒ Agree ☐ Disagree

Comments/Action Plan/Time Frame:

The Chief Technology Officer will enhance the project governance and project management framework by:

a. Developing a clear RACI matrix for each project. It will ensure that stakeholders' roles and responsibilities are clearly defined and there is proper stakeholder representation from the project initiation stage, including the City Clerk and Chief Information Security Officer for privacy and security impacts – **Q3 2021**
b. Ensuring the PRT Gating Model includes a support transition plan from 'project' to 'operations' for all projects at last gate before moving to production stage – **Q3 2021**
c. Please refer to response: a.
d. Developing criteria to determine projects with high risks that have not been mitigated prior to moving to production and the mechanics for escalating to the Senior Leadership Team (SLT) – **Q3 2021**

Expected implementation date: **Q3 2021**

Recommendation 6: City Council request the Chief Technology Officer to enhance project management framework by including a review of internal controls for systems that involve financial transactions. The Controller's Office or Internal Audit should be involved in the review of user roles in relation to financial transaction processing to ensure appropriate segregation of duties is maintained for all user roles.

Management Response: ☒ Agree ☐ Disagree

Comments/Action Plan/Time Frame:

The Chief Technology Officer will enhance the project management framework by ensuring that projects that involve financial transactions have a specific review of internal controls including segregation of duties, in consultation with the Controller's Office or Internal Audit – **Q3 2021**

Expected implementation date: **Q3 2021**

Recommendation 7: City Council request the Chief Technology Officer, improve the user permissions framework of the Human Resources application. This includes:

a. Conducting the cybersecurity and information privacy review of the various roles created in the HR system.
b. Reviewing the users with a Super Administrator role and limiting the number of users with that role considering the industry's best practices and professional bodies.
c. Ensuring that user access roles are designed with cybersecurity and information privacy in mind. The access roles should be provided to users on a 'need to have' basis.
d. Defining a process for the approval of access roles for support staff. Instead of providing Super Administrator access, the support staff should be provided access on a 'need to have' basis.
e. Eliminating the use of generic and anonymous accounts. If these roles are needed as an exception for operational reasons, detailed monitoring and logging procedures should be developed and implemented for these roles.

In addition, the review of elevated access roles, use of generic or anonymous users should be extended to the SAP enterprise application.

Management Response: ☒ Agree ☐ Disagree

Comments/Action Plan/Time Frame:

The Chief Technology Officer will improve the user permissions framework of the Human Resources application by:

a. Conducting a cybersecurity and information privacy review and update of all roles created in the HR system, not only those identified in the previous privacy incidents – **Q4 2021**
b. Conducting a review of accounts with Super Administrator access and limiting the number of users with that role, using least privileged access principles and considering the industry's best practices and respective professional bodies – **Q3 2021**
c. Ensuring that user roles are designed based on least privileged access principles where possible, and considering the industry's best practices and respective professional bodies – **Q4 2021**
d. Defining a process for the approval of access roles for support staff based on least privileged access principles where possible, and considering the industry's best practices and respective professional bodies – **Q4 2021**

e. Eliminating the use of generic and anonymous accounts for operational support where possible. If these roles are needed as an exception for operational reasons, a risk-based approach will be adopted to limit use, considering the industry's best practices and respective professional bodies – **Q3 2021**

In addition, a review of elevated access roles and use of generic or anonymous users in the SAP enterprise application will be considered, with the intent of adopting a risk-based approach to limit use.

Expected implementation date: **Q4 2021**

Recommendation 8: City Council request the Chief Technology Officer to develop standards and minimum criteria for logging user activity details for IT systems. Steps include but are not limited to:

a. Ensuring user access logs capture account activity for users with elevated access, such as, users with Super Administrator or Divisional Administrator roles.
b. Implementing a user activity review process for roles with elevated access on a periodic basis to ensure access is aligned with the role.

Management Response: ☒ Agree ☐ Disagree

Comments/Action Plan/Time Frame:

The Chief Technology Officer will develop standards and minimum criteria for logging user activity details for IT systems by:

a. This capability does not currently exist in the system. Technology Services Division to request that this capability be added to the system product roadmap – Request to vendor be submitted by **Q2 2021**
b. Implementing a process to conduct monthly reviews for roles with elevated access to ensure alignment with the role – **Q3 2021**

Expected implementation date: **Q4 2021**

Recommendation 9: City Council request the Chief Technology Officer to implement a process to ensure comprehensive system testing and user acceptance testing is part of the overall IT project management methodology. This includes:

a. Assigning staff having subject matter expertise in Technology Services Division or Office of the Chief Information Security Officer to review the test scope, test cases and test cycle defect management.
b. Ensuring that user acceptance testing is started early in the project stage and performed by respective divisions (users). In situations where, testing is performed by staff other than

the User Division, the test results must be formally approved by the respective Division Lead contact on the project.

c. Ensuring each test cycle go through a formal approval process and mandatory security testing prior to commencing the next test cycle.

Management Response: ☒ Agree ☐ Disagree

Comments/Action Plan/Time Frame:

The Chief Technology Officer will implement a process to ensure comprehensive system testing and user acceptance testing is part of the overall IT project management methodology by:

a. Ensuring that all projects have a defined test plan aligned with the appropriate expertise in Technology Services Division – **Q4 2021**
b. Ensuring that all user acceptance testing has Divisional sign-off – **Q4 2021**
c. Ensuring that the test cycle proceeds through a formal process to meet the assigned security testing – **Q4 2021**

Expected implementation date: **Q4 2021**

Recommendation 10: City Council request the Chief Technology Officer to research options to automate the move of configuration of systems from testing to the production environment.

Alternatively, include a peer review (Quality Assurance) to verify post implementation configuration in the system after it has been moved to the production environment.

Management Response: ☒ Agree ☐ Disagree

Comments/Action Plan/Time Frame:

The Chief Technology Officer will research options related to the move of configuration of systems from testing to the production environment to improve the migration of configurations into production. Based on the options evaluation, this may be an automated tool or an additional manual post implementation peer review verification step – **Q3 2021**

Expected implementation date: **Q3 2021**

Appendix 2: Previous Auditor General's Reports on IT Security (2016-2020)

1. 2020: City's Critical Infrastructure Systems

(i) Cyber Safety - Critical Infrastructure Systems: Toronto Water SCADA System, January 2020
https://www.toronto.ca/legdocs/mmis/2020/au/bgrd/backgroundfile-145342.pdf

(ii) Cyber Safety - Critical Infrastructure Systems: Toronto Water SCADA System - Recommendations Implementation Progress by Management, June 2020
https://www.toronto.ca/legdocs/mmis/2020/cc/bgrd/backgroundfile-148217.pdf

2. 2016-2019: Ransomware Attacks' Incident Management, IT Vulnerability Assessments, Penetration Testing and IT Infrastructure Reviews

(i) Establishment of City-Wide Cybersecurity Breach Incident Management Procedures Required, June 2019
https://www.toronto.ca/legdocs/mmis/2019/au/bgrd/backgroundfile-135368.pdf

(ii) Audit of Information Technology Vulnerability and Penetration Testing – Phase 1: External Penetration Testing, February 2016
https://www.toronto.ca/legdocs/mmis/2016/au/bgrd/backgroundfile-90751.pdf

(iii) Audit of Information Technology Vulnerability and Penetration Testing – Phase II: Internal Penetration Testing, Part 1 – Accessibility of Network and Servers, October 2016
https://www.toronto.ca/legdocs/mmis/2016/au/bgrd/backgroundfile-97617.pdf

(iv) Information Technology Vulnerability Assessment and Penetration Testing - Wrap-up of Phase I and Phase II, March 2017
https://www.toronto.ca/legdocs/mmis/2017/au/bgrd/backgroundfile-101892.pdf

(v) IT Infrastructure and IT Asset Management Review: Phase 1: Establishing an Information Technology Roadmap to Guide the Way Forward for Infrastructure and Asset Management, January 2018
https://www.toronto.ca/legdocs/mmis/2018/au/bgrd/backgroundfile-112385.pdf

(vi) Information Technology Infrastructure and Asset Management Review: Phase 2: Establishing Processes for Improved Due Diligence, Monitoring and Reporting for Effective IT Projects and Asset Management, June 2018
https://www.toronto.ca/legdocs/mmis/2018/au/bgrd/backgroundfile-118363.pdf