AUDITOR GENERAL TORONTO

REVIEW AT A GLANCE

Information Technology Projects Implementation: Information Privacy and Cybersecurity Review of Human Resource System

WHY THIS REVIEW MATTERS

In early 2020, Auditor General became aware of a security incident in the City's HR system through a Fraud Hotline complaint.

The HR system collects and stores significant information relating to users, such as employees and elected officials.

Given the importance of information privacy and cybersecurity, the Auditor General immediately initiated a review of the system implementation process in the context of the overall cybersecurity and information privacy controls at the City.

BY THE NUMBERS

- The System has over 40,000 users
- 15 risks in the Threat Risk Assessment document were not fully mitigated prior to the launch of the system
- 3 security incidents occurred during implementation
- 10 months delay in setting up remedial action plan from the 1st security incident that occurred in September 2019
- 90 users had Super Administrator access
- 12 anonymous accounts had super Administrator access
- 42 roles assigned without completing review of controls

BACKGROUND

In 2017, the City initiated the implementation of an integrated human resource management solution. The system includes management of organizational structures, employee data and enables enterprise-wide workflows.

The Auditor General, on receipt of a Fraud Hotline complaint relating to inappropriate access, undertook a review of the information privacy and cyber security of the HR system.

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

WHAT WE FOUND

The results of our review identified areas that need strengthening to address cybersecurity and information privacy controls.

Summary of Findings

Our review noted the following:

A – Project Governance

The Governance Framework needs to be strengthened:

- Risks are not fully evaluated from project inception to post-implementation
- Privacy and security by design principles need to be implemented
- Key stakeholders need to be involved in all phases of the project
- Roles and responsibilities need to be clearly defined
- Project team needs to comply with project management approval process

B – User Access Controls and Activity Logging

- We found large number of users with Super Administrator access to the system
- Industry best practices suggest minimizing the number of users with high privileged access
- Some anonymous accounts were created for support roles and shared among users.
- The system was not configured to fully track and monitor user activities for high privileged users.

C –System Testing and Quality Assurance review

- Lack of comprehensive user acceptance testing
- Final testing results were "conditionally" approved
- Quality assurance review (post implementation validation) was not completed.

HOW RECOMMENDATIONS WILL BENEFIT THE CITY

The Auditor General has made 10 recommendations to improve cybersecurity and information privacy controls. Implementation of recommendations will strengthen project governance and improved controls to address cybersecurity and information privacy risks when implementing large technology systems.