REPORT FOR ACTION

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

Date: February 3, 2021
To: Audit Committee
From: Auditor General
Wards: All

SUMMARY

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 human resources information for employees and elected officials. Because of this, it is extremely important that the system has strong cybersecurity and privacy controls in place.

In early 2020, the Auditor General became aware of a cybersecurity incident related to the implementation of this new system. 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. Since 2015, the Auditor General has performed a number of audits of the City's IT infrastructure and critical systems, 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.

The objective of this review was to assess the implementation of information privacy and cybersecurity controls of this new HR system. The findings are categorized into three areas where the City needs to improve cybersecurity and information privacy:

- Strengthening project governance
- Improving user access controls and activity logging processes
- Strengthening on end-to-end system testing including user acceptance testing

We have made 10 recommendations to address the weaknesses identified during our review. Implementation of our recommendations will strengthen project governance and improved controls to address cybersecurity and information privacy risks when implementing large technology systems.

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

CONCLUSION

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.

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. The review will 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.

RECOMMENDATIONS

The Auditor General recommends that:

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”

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[1].

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.

[1] 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)

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

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.

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.

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.

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.

FINANCIAL IMPACT

Implementing the recommendations in this report will strengthen both cybersecurity and privacy controls in the City.

The extent of costs and resources needed to implement the recommendations is not determinable at this time. The investment needed to improve controls that manage and respond to cyber threats likely offsets the costs that could result from security breaches, such as recovery of infrastructure systems, data recovery/cleanup, financial loss, reputational damage, fines and litigation.

DECISION HISTORY

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 decided to immediately initiate a review of the system implementation process of the HR system, in the context of overall information security at the City.

COMMENTS

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.

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

The attached report provides Audit Committee with detailed results and recommendations together with management's response. Management has agreed to implement all 10 recommendations.

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.

CONTACT

Syed Ali, Audit Director, IT & Strategy, Auditor General's Office
Tel: 416-392-8438, Fax: 416-392-3754, Email: Syed.Ali@toronto.ca

Suzanna Chan, Audit Manager, Auditor General's Office
Tel: 416-392-8033, Fax: 416-392-3754, Email: Suzanna.Chan@toronto.ca

SIGNATURE

Beverly Romeo-Beehler
Auditor General

ATTACHMENT

Attachment 1 - Information Technology Projects Implementation: Information Privacy and Cybersecurity Review of Human Resource System