Centralized Identity and Access Management

Background

Centralized Identity and Access Management (IAM) is defined as all processes and technological tools used in the centralized management of users and their access rights to information systems and applications. IAM provides all users, internal and external, appropriate access in a timely manner, while reducing the number of identifiers and passwords that need to be remembered. IAM control mechanisms are adapted to the security and sensitivity levels of the information being accessed. To achieve this, organizations adopt standards and industry best practices. They enable the implementation of standardized policies and control mechanisms that ensure the protection of data.

In 2016, the Ville de Montréal (the City) has launched two projects to meet the IAM needs of citizens and employees, they're known as GIA Citoyens and GIA Employés, respectively. The GIA Citoyens project is currently under the responsibility of the Division solutions numériques of the Service des technologies de l'information (STI), while the GIA Employés project comes under the responsibility of the STI's Direction sécurité de l'information. Because of the departure of key employees and changes in their duties and responsibilities, the GIA Employés project is being relaunched.

In the meantime, the GIA Employés serves about 30,200 employee accounts, 1,700 external user accounts, 560 application accounts and integrates 125 applications. As for the GIA Citoyens, it serves more than 255,000 citizen accounts and integrates 70 applications.

Purpose of the Audit

To determine whether the IAM process and its control mechanisms implemented by the City provide assurance that they do not present any major risk to the confidentiality, integrity and availability of data.

Results

In the case of GIA Citoyens, we can conclude that the process and control mechanisms put in place do not present any major risk to the confidentiality, integrity and availability of data. However, we believe that ongoing work to adopt the Pan-Canadian Trust Framework (PCTF) for digital identities must continue. Note that the Trust Framework defines and standardizes processes and specifies privacy requirements, which would optimize the security of data and services available to citizens.

For GIA Employés, given that the project is being relaunched, our findings do not allow us to conclude that this IAM provides adequate risk management for data confidentiality, integrity and availability. We identified gaps in the areas of governance, definition of roles and responsibilities, project strategy, as well as in risk analysis and process documentation. Moreover, the technological tools currently in use will be replaced. Therefore, there is no IAM process yet. Rather, the controls in place respond to decentralized administrative mechanisms.

Main Findings

Governance

GIA Citoyens:

- The IAM strategy is properly documented;
- The process owner is not formally identified and the roles and responsibilities are not fully documented;
- The risk analysis is not completed;
- Assurance levels, which establish security requirements based on the confidentiality level of the information to be accessed, are not formally established.

GIA Employés:

- The process owner is not formally identified and the roles and responsibilities are not properly defined. Moreover, management frameworks are not finalized;
- The GIA Employés project has shortcomings regarding the active involvement of the Comité de sécurité de l'information (CSI) and business units, the inclusion of all types of users, the analysis of the current context (processes and technologies), the documentation of business requirements, the standardization of phases and deliverables, as well as the absence of the target architecture;
- The risk analysis and proposed controls do not meet the requirements of an IAM;
- The assurance levels, which establish security requirements in accordance with the confidentiality level of the information being accessed, are not yet formally established.

User Management (Identities)

- Citizen identity management is adequate apart from the lack of an account deletion mechanism.

Authentication Management

- The GIA Employés and GIA Citoyens authentication are not adapted to the different confidentiality levels of the information being accessed.

Access Management

- Citizen access management meets the least-privilege and need-to-know criteria;
- The process for periodic review of citizens' access is not in place.

Integration of Applications into IAM

- This process is adequate in GIA Citoyens. However, teams must ensure that the applications integrated into GIA Citoyens are also integrated into the Dossier citoyen intégré (DCI) and that any exceptions are formally justified.

In addition to these results, we formulated various recommendations to the business units, which are presented in the following pages. The business units concerned were given the opportunity to agree to these recommendations.