Gestion centralisée des identités et des accès

Mise en contexte

La Gestion centralisée des identités et des accès (GIA) se définit comme un ensemble des processus et des outils mis en œuvre pour une gestion centralisée des utilisateurs et de leurs droits d'accès aux systèmes d'information et aux applications. Elle permet de fournir à tous les utilisateurs, internes et externes, les accès appropriés en temps opportun, tout en réduisant le nombre d'identifiants et de mots de passe à retenir. Les mécanismes de contrôle de la GIA sont adaptés au degré de sécurité et de sensibilité des informations à accéder. Pour ce faire, les organisations adoptent des normes et de meilleures pratiques du marché. Cela permet l'implantation de politiques et de mécanismes de contrôle uniformisés et assure la protection des données.

La Ville de Montréal (la Ville) a déclenché deux projets pour répondre aux besoins de la GIA des employés et des citoyens. La GIA Citoyens a débuté en 2016 et elle est actuellement sous la responsabilité de la Division solutions numériques du Service des technologies de l'information (STI). Le projet de la GIA Employés est sous la responsabilité de la Direction sécurité de l'information du STI. La GIA Employés a débuté en 2016. Cependant, à la suite des départs d'employés clés et des changements de responsabilités, ce projet est en redémarrage.

Entretemps, la GIA Employés dessert autour de 30 200 comptes d'employés, 1 700 comptes d'utilisateurs externes, 560 comptes pour les applications et intègre 125 applications. Quant à la GIA Citoyens, elle dessert plus de 255 000 comptes des citoyennes et de citoyens et 70 applications y sont intégrées.

Objectif de l'audit

Déterminer si le processus de GIA et ses mécanismes de contrôle mis en place au sein de la Ville permettent de s'assurer que ceux-ci ne présentent aucun risque majeur de confidentialité, d'intégrité et de disponibilité des données.

Résultats

Pour la GIA Citoyens, nous pouvons conclure que le processus et les mécanismes de contrôle mis en place ne présentent pas de risque majeur de confidentialité, d'intégrité et de disponibilité des données. Cependant, nous sommes d'avis que les travaux en cours doivent se poursuivre pour l'adoption du cadre de confiance pancanadien pour les identités numériques. À noter que ce cadre de confiance définit et uniformise les processus et spécifie les exigences en matière de protection des renseignements personnels, ce qui optimiserait la sécurité des données et des services offerts aux citoyens.

Pour le volet de la GIA Employés, comme le projet est en redémarrage, nos constats ne permettent pas de conclure que cette GIA assure une gestion de risque adéquate concernant la confidentialité, l'intégrité et la disponibilité des données. Nous avons relevé des lacunes au niveau de la gouvernance, de la définition des rôles et des responsabilités, de la stratégie du projet ainsi que dans l'analyse de risques et la documentation des processus. De plus, les outils implantés seront remplacés. Par conséquent, il n'y a pas encore de processus de GIA. Les contrôles en place répondent plutôt à des mécanismes décentralisés et administratifs.

Principaux constats

Gouvernance

Concernant la GIA Citoyens :

- La stratégie de GIA est adéquatement documentée;
- Le propriétaire du processus n'est pas formellement identifié et les rôles et les responsabilités ne sont pas complètement documentés;
- L'analyse de risques n'est pas complétée;
- Les niveaux d'assurance, qui établissent les exigences de sécurité en fonction du degré de confidentialité des informations à accéder, ne sont pas formellement établis.

Concernant la GIA Employés :

- Le propriétaire du processus n'est pas formellement identifié et les rôles et les responsabilités ne sont pas adéquatement définis. Également, les encadrements ne sont pas finalisés;
- Pour le projet de la GIA Employés, des lacunes sont présentes quant à l'implication active du Comité de sécurité de l'information (CSI) et des unités d'affaires, l'inclusion de tous les types d'utilisateurs, l'analyse du contexte actuel (processus et technologique), la documentation de besoins d'affaires, l'harmonisation des phases et des livrables et l'absence d'architecture cible;
- L'analyse de risques et les contrôles proposés ne répondent pas à une GIA;
- Les niveaux d'assurance, qui établissent les exigences de sécurité en fonction du degré de confidentialité des informations à accéder, ne sont pas encore formellement établis.

Gestion des utilisateurs (identités)

- La gestion des identités des citoyens est adéquate mis à part l'absence d'un mécanisme pour la suppression de comptes.

Gestion de l'authentification

- L'authentification de la GIA Employés et de la GIA Citoyens n'est pas adaptée aux différents niveaux de confidentialité des informations à accéder.

Gestion des accès

- La gestion des accès des citoyens répond aux critères de moindre privilège et du besoin de savoir;
- Un processus de révision périodique des accès des citoyens centralisé n'est pas en place.

Intégration des applications dans la GIA

- Dans la GIA Citoyens, ce processus est adéquat. Cependant, les équipes doivent s'assurer que les applications intégrées à la GIA Citoyens le sont aussi au Dossier citoyen intégré (DCI) et que tout écart est formellement justifié.

En marge de ces résultats, nous avons formulé différentes recommandations aux unités d'affaires qui sont présentées dans les pages suivantes. Ces unités d'affaires ont eu l'opportunité de donner leur accord relativement aux recommandations.