3.3.

Gestion centralisée des identités et des accès

Service des technologies de l'information

Le 8 février 2022

RAPPORT ANNUEL 2021
Bureau du vérificateur général de la Ville de Montréal

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.

Liste des sigles

CCIAN	Conseil canadien de l'identification et de l'authentification numériques
CISO	Chef de la sécurité de l'information (*Chief Information Security Officer*)
CSI	Comité de sécurité de l'information
DCI	Dossier citoyen intégré
GIA	Gestion centralisée des identités et des accès
RASCI	Responsable, Approbateur, Soutien, Consulté et Informé
SRH	Service des ressources humaines
STI	Service des technologies de l'information

Table des matières

1. Contexte

Les organismes de grande envergure comme la Ville de Montréal (la Ville) ont de multiples ressources informationnelles qui servent de nombreux corps de métiers et de fonctions administratives. Pour accéder aux ressources, souvent un utilisateur cumule une multitude de mots de passe. Cela peut entraîner une dégradation de la sécurité, car les utilisateurs ont tendance à oublier les consignes de sécurité et réutilisent les mêmes mots de passe d'une application à l'autre.

La protection des accès aux ressources informationnelles est encore plus importante aujourd'hui à cause de l'essor du télétravail. Les ordinateurs des utilisateurs sortent des limites traditionnelles du réseau de l'entité. Un environnement non suffisamment sécurisé pourrait être la cible des cybercriminels et souvent un identifiant compromis constitue la porte d'entrée à d'autres attaques plus dommageables comme un vol de données massif ou des rançongiciels.

Pour rendre plus sécuritaire l'environnement informatique, l'entité doit instaurer une Gestion centralisée des identités et des accès (GIA). La GIA se définit comme un ensemble de processus et d'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. Les mécanismes de contrôle de la GIA sont adaptés au degré de sécurité et de sensibilité des informations à accéder. Ainsi, l'entité adopte des normes et de meilleures pratiques du marché qui proposent des politiques et des mécanismes de contrôle uniformisés pour la protection des identités et des accès aux données.

Parmi les avantages que la GIA fournit à une organisation se trouvent :

- l'amélioration de l'expérience utilisateur, en réduisant le nombre d'identifiants et de mots de passe à retenir pour l'accès aux actifs informationnels;
- une réduction de la surcharge administrative concernant la gestion de comptes, grâce à des outils de libre-service et des processus automatisés d'autorisation, d'approbation, de modification et de révocation des accès;
- l'optimisation de la sécurité de comptes et des actifs informationnels, avec l'implantation de mécanismes d'authentification multifacteur et de politiques appliquées en fonction de risques;
- l'uniformisation des profils d'accès qui respectent les meilleures pratiques, tels le principe du moindre privilège, le besoin de savoir et la séparation de tâches incompatibles;

- des mécanismes simplifiés, offerts aux responsables des actifs informationnels, pour la révision périodique des accès;
- des mécanismes d'alertes et de surveillance permettant la détection et le traitement des accès non autorisés.

1.1. Portrait de la Gestion centralisée des identités et des accès à la Ville de Montréal

Dans un effort pour normaliser les exigences à respecter lors de l'accès à l'information non publique relevant de la responsabilité de la Ville, cette dernière a émis une directive et un standard concernant la gestion des accès logiques. Ces encadrements visent tous les employés et les individus provenant de firmes externes ou partenaires ayant accès à ces informations. La directive, pour sa part, mentionne les responsabilités de principales parties prenantes, notamment le Comité de sécurité de l'information (CSI) et le Chef de la sécurité de l'information (*Chief Information Security Officer*) (CISO). Le premier veille à l'adoption d'une approche transversale de gestion des accès logiques, commune aux unités d'affaires et adaptée à leur contexte d'affaires. Cela assurerait une gestion adéquate des risques afférents. Le deuxième doit, entre autres, délivrer et administrer les identifiants, ainsi qu'implanter des mesures de sécurité pour mitiger les risques reliés aux accès logiques.

En ce qui concerne les solutions en place, la Ville a déclenché deux projets pour répondre aux besoins de la GIA des employés et des citoyens. Ce qui a mené à l'implantation de deux solutions distinctes, une pour les citoyens et une autre pour les employés. La GIA Citoyens, connue comme « l'identité numérique des citoyens » était une initiative découlant du projet « Présence numérique – Fondation ». Il a débuté en 2016 sous la responsabilité du « Bureau de l'expérience citoyenne ». Lors de l'abolition de ce dernier, la Division solutions numériques du Service des technologies de l'information (STI) a pris la relève pour sa gestion. D'autre part, le projet de la GIA Employés est sous la responsabilité de la Direction sécurité de l'information du STI. Cette initiative fait partie du programme de sécurité et de continuité TI et a débuté en 2016. Cependant, à la suite des départs d'employés clés et des changements de responsabilités, ce projet est en redémarrage.

L'approche du projet « l'identité numérique des citoyens » était centrée sur les citoyens et l'amélioration de services offerts. Pour mener à terme ce projet, la Ville a implanté un portail permettant aux citoyens de créer un compte et de bénéficier de services en ligne. Jusqu'à présent, la GIA Citoyens dessert plus de 255 000 comptes des citoyennes et de citoyens et 70 applications y sont intégrées.

Pour ce qui est de la GIA Employés, le projet a adopté une approche plus technologique. L'équipe a priorisé le rehaussement des accès et de l'authentification. Cependant, en raison d'enjeux technologiques et financiers, les outils choisis pour le projet sont à remplacer. Entretemps, les outils actuels desservent plus de 30 200 comptes d'employés, environ 1 700 comptes d'utilisateurs externes et près de 560 comptes pour des applications. En somme,

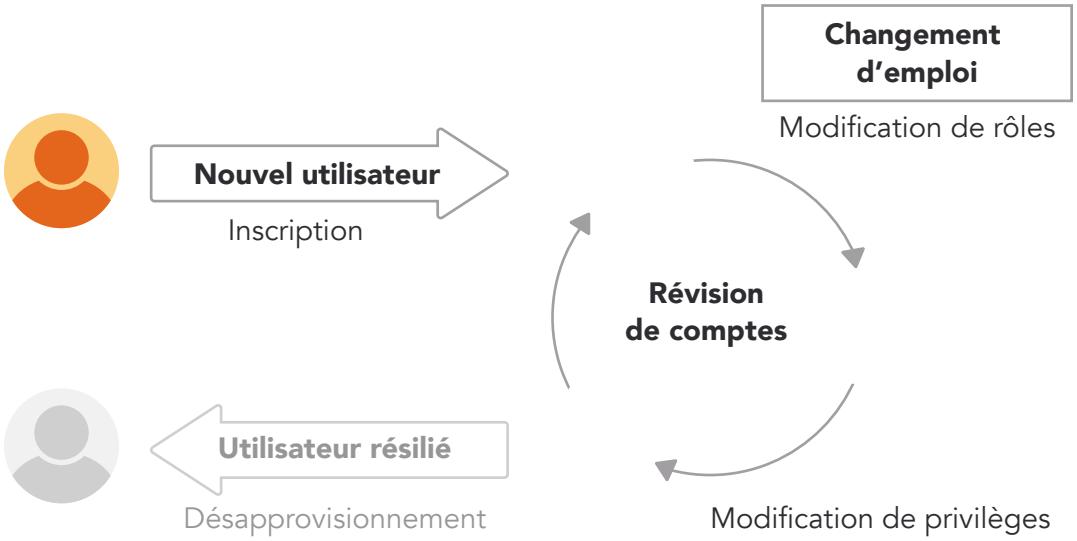
125 applications y sont intégrées. Les processus de GIA reposent actuellement dans des procédures administratives, décentralisées et sous la responsabilité de chaque unité d'affaires. Les travaux concernant les besoins d'affaires, les processus et le choix des standards à adopter devraient être entrepris en 2022. De plus, des solutions intermédiaires seront déployées.

1.2. Cycle de vie des comptes

Dans cette section, nous décrivons de façon théorique les divers éléments qui composent le cycle de vie d'un compte d'utilisateur :

FIGURE 1

Cycle de vie d'un compte utilisateur



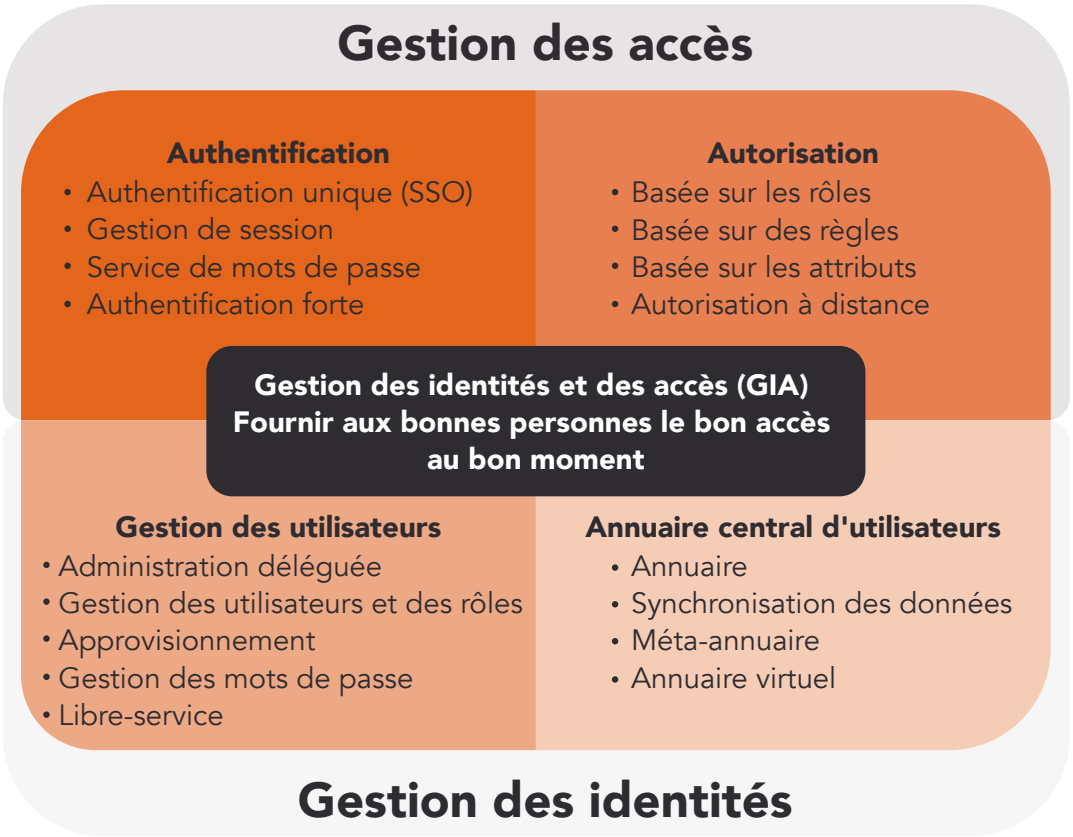
- *L'inscription :* Un compte est créé lorsqu'un nouvel utilisateur arrive. La vérification de l'identité de ce nouvel utilisateur répond aux exigences de sécurité des actifs à accéder. Par exemple, pour s'inscrire à un site web informatif, un compte courriel suffit; par contre, l'accès à un actif hautement confidentiel pourrait exiger, par exemple, une vérification du casier judiciaire de l'utilisateur;
- *L'octroi des accès :* Une fois le compte créé, des habilitations lui sont octroyées pour accéder aux actifs requis. Tout octroi d'accès répond à un processus d'approbation, automatisé ou manuel. L'assignation de rôles est une façon simplifiée d'octroi des accès. Par exemple, le rôle de comptable définit les accès aux systèmes de finances requis et sera automatiquement octroyé aux comptables engagés;
- *La modification des accès :* Lorsque les besoins d'accès changent, soit en raison d'un changement d'emploi, de rôle, ou des fonctions, ainsi que lors de l'ajout ou retrait des actifs, il faut modifier les privilèges octroyés. Ces modifications requièrent aussi une approbation au préalable;

- *La révision et la surveillance des accès* : Une révision des accès est effectuée périodiquement par les propriétaires des actifs afin de s'assurer qu'il n'y a pas des utilisateurs non autorisés. La surveillance des accès est réalisée en continu pour veiller à une utilisation adéquate des accès et à la détection des incidents;
- *Le désapprovisionnement* : Lorsqu'un utilisateur part ou que son compte n'est plus requis, les responsables des accès demandent la fermeture de son compte, ce qui mène à sa résiliation. Ainsi, les comptes résiliés sont détruits en suivant les normes de conservation de l'information de chaque organisation.

La GIA permet l'implantation simplifiée et sécuritaire du cycle de vie de comptes présenté précédemment. Pour ce faire, des processus et des composantes technologiques sont mis en place. Ils couvrent les quatre catégories suivantes (voir la figure 2) :

FIGURE 2

Cadre de la Gestion centralisée des identités et des accès



- ***La gestion des identités :***
  - ***La gestion des utilisateurs*** : Elle permet de gérer les comptes et les rôles des identités dès leur création jusqu'à leur désactivation ou destruction. Cela inclut l'approvisionnement des utilisateurs, la gestion de mots de passe, l'octroi et la maintenance de profils, ainsi que la mise en place des outils en libre-service. Ces derniers simplifient la gestion des identités grâce à des fonctionnalités tels les profils autogérés et la réinitialisation automatique des mécanismes d'authentification multifacteur et des mots de passe;
  - ***L'annuaire central des utilisateurs*** : l'annuaire central présente une vue agrégée des identités d'une entreprise. Il fournit des informations d'identité à d'autres services ainsi qu'un service de vérification des informations d'identification soumises par les clients. Étant une infrastructure qui centralise l'ensemble de comptes et des droits des utilisateurs pour toutes les applications, il simplifie son exploitation et facilite les accès aux utilisateurs;

- ***La gestion des accès :***
  - ***L'authentification*** : L'authentification est la fonctionnalité à travers laquelle un utilisateur fournit des informations d'identification suffisantes pour obtenir un accès initial à un système ou à une ressource particulière. Cette authentification peut être réalisée à l'aide d'un ou de plusieurs facteurs d'authentification tels des mots de passe, des jetons, des messages texte, etc. Une fois qu'un utilisateur est authentifié, une session est créée et référencée pendant l'interaction entre l'utilisateur et le système. Cette session est verrouillée lorsque l'utilisateur se déconnecte ou lorsque d'autres événements sont déclenchés (p. ex. un temps d'inactivité de l'utilisateur);
  - ***L'autorisation*** : L'autorisation est la fonctionnalité qui détermine si un utilisateur est autorisé à accéder à une ressource particulière. De façon générale, l'autorisation est gérée en fonction des rôles préétablis. La GIA offre aussi des mécanismes pour simplifier la révision périodique des accès, la détection des habilitations en conflit ainsi que le retrait automatique des accès lors du départ d'un utilisateur, d'un changement de rôle, d'une suspension, etc.

2. Objectif de l'audit et portée des travaux

En vertu des dispositions de la *Loi sur les cités et villes* (LCV), nous avons réalisé une mission d'audit de performance portant sur la GIA. Nous avons réalisé cette mission conformément à la *Norme canadienne de missions de certification* (NCMC) 3001, du *Manuel de CPA Canada – Certification*.

Le présent audit avait pour objectif d'évaluer le processus de la GIA et ses mécanismes de contrôle mis en place au sein de la Ville, permettant de s'assurer que ceux-ci ne présentent aucun risque majeur de confidentialité, d'intégrité et de disponibilité des données.

La responsabilité du vérificateur général de la Ville de Montréal consiste à fournir une conclusion sur l'objectif de l'audit. Pour ce faire, nous avons recueilli des éléments probants suffisants et appropriés pour fonder notre conclusion et pour obtenir un niveau d'assurance raisonnable. Notre évaluation est basée sur les critères que nous avons jugés valables dans les circonstances. Ces derniers sont exposés à l'annexe 5.1.

Le vérificateur général de la Ville de Montréal applique la *Norme canadienne de contrôle qualité* (NCCQ 1), du *Manuel de CPA Canada – Certification* et, en conséquence, maintient un système de contrôle qualité exhaustif qui comprend des politiques et des procédures documentées en ce qui concerne la conformité aux règles de déontologie, aux normes professionnelles et aux exigences légales et réglementaires applicables. De plus, il se conforme aux règles sur l'indépendance et aux autres règles de déontologie du *Code de déontologie des comptables professionnels agréés*, lesquelles reposent sur les principes fondamentaux d'intégrité, de compétence professionnelle et de diligence, de confidentialité et de conduite professionnelle.

Notre audit a été réalisé pour la période d'avril à novembre 2021. Il a consisté à effectuer des entrevues auprès du personnel, à examiner divers documents et à réaliser les sondages que nous avons jugés appropriés en vue d'obtenir l'information probante nécessaire. Nous avons toutefois tenu compte d'informations qui nous ont été transmises jusqu'au 8 février 2022.

À la fin de nos travaux, un projet de rapport d'audit a été présenté, aux fins de discussions, aux gestionnaires concernés au sein de l'unité d'affaires auditée pour l'obtention de plans d'action et d'échéanciers pour leurs mises en œuvre.

3. Résultats de l'audit

3.1. Gouvernance

3.1.1. Rôles, responsabilités et responsable du processus

Une saine gouvernance entourant la GIA consiste à définir les rôles et les responsabilités des différentes parties prenantes impliquées dans chaque tâche reliée à sa gestion. Cela se formalise dans une matrice de responsabilités de type RASCI (Responsable, Approbateur, Soutien, Consulté et Informé).

De plus, pour un processus de cette envergure, il est important de définir qui sera la personne responsable de celui-ci, permettant une imputabilité claire pour chaque action nécessitant une chaîne de validation. Le propriétaire du processus est le responsable de la gestion opérationnelle de celui-ci. Il doit être impliqué pour chaque changement majeur et pour chaque migration applicative.

GIA Employés

Dans les documents audités, nous retrouvons plusieurs matrices de responsabilités de type RASCI pour la gestion de certains outils de GIA.

Seulement la matrice de responsabilités de type RASCI pour l'outil d'authentification unique et pour l'authentification forte à deux facteurs[1] est formellement approuvée.

En révisant le contenu des autres matrices de responsabilités de type RASCI, nous avons relevé les lacunes suivantes :

- Il n'y a pas de matrice de responsabilités de type RASCI qui couvre la GIA dans son ensemble;
- Les tâches définies sont surtout reliées aux outils technologiques;
- Pour une majorité de tâches, l'approbateur n'est pas indiqué;
- Les rôles et les responsabilités des autres parties prenantes ne sont pas spécifiés (p. ex. le Service des ressources humaines (SRH), les utilisateurs, les développeurs d'applications, les autres unités administratives).

La directive de gestion des accès de la Ville mentionne les responsables suivants :

- Le CSI pour l'adoption d'une approche transversale de gestion des accès;
- Le CISO pour la gestion des identités et leur sécurité.

[1] Authentification à deux facteurs : authentification par laquelle l'utilisateur doit fournir deux éléments appartenant à deux facteurs d'authentification distincts, p. ex. un mot de passe et un jeton installé sur un téléphone.
(Source : Office québécois de la langue française)

Malgré ce que la directive stipule, nous avons noté qu'il y a de la confusion au niveau des responsabilités reliées à la GIA. Lorsque nous avons rencontré l'équipe de la sécurité, elle nous a informés, entre autres, que :

- la gestion des identités était sous la responsabilité du SRH;
- la gestion des accès de consultants était sous la responsabilité du bureau de projets au STI;
- le Centre de services TI était responsable des demandes de service d'accès qu'il traite;
- chaque unité d'affaires était responsable de gérer ses accès aux applications.

Cependant, lors de nos rencontres avec le SRH, le bureau de projets et le Centre de services, ils ne considéraient pas que cela soit sous leur responsabilité, même s'ils ont un rôle à jouer.

Nous concluons que les rôles et les responsabilités établis dans la directive ne sont pas adéquatement communiqués. De plus, il y a un manquement dans la définition, la documentation et l'approbation des rôles et responsabilités pour l'ensemble du processus de la GIA.

Le manque d'identification formelle d'un propriétaire ainsi que des lacunes dans la définition des rôles et des responsabilités reliés à la GIA pourraient causer des dysfonctionnements comme :

- une absence de prise de responsabilité sur les décisions reliées à la GIA;
- une collaboration inefficace entre les équipes (p. ex. les utilisateurs redirigés vers les mauvaises équipes pour la gestion des accès ou d'un incident);
- des octrois de privilèges applicatifs sans validation au préalable;
- des tâches non exécutées, des omissions et des actions inégales quant à la gestion de la GIA.

3.1.1.A. Recommandation

Nous recommandons à la Direction sécurité de l'information du Service des technologies de l'information de définir formellement le propriétaire du processus de la Gestion centralisée des identités et des accès.

3.1.1.B. Recommandation

Nous recommandons à la Direction sécurité de l'information du Service des technologies de l'information de communiquer les rôles et les responsabilités concernant la Directive de gestion des accès aux différentes parties prenantes.

3.1.1.C. Recommandation

Nous recommandons à la Direction sécurité de l'information du Service des technologies de l'information de documenter, approuver et diffuser les rôles et les responsabilités reliées à la Gestion centralisée des identités et des accès dans son ensemble.

GIA Citoyens

Lors de nos tests d'audit, nous avons constaté :

- que les rôles et les responsabilités sont bien connus des principaux intervenants en poste. Cela a été confirmé lors des entrevues et par la collecte de documents reliés aux processus et des outils en place;
- qu'une matrice de responsabilités de type RASCI a été définie et couvre le développement, le soutien, l'évolution des technologies, ainsi que les communications aux citoyens;
- que les différentes parties prenantes ont été identifiées;
- que le propriétaire de la GIA Citoyens n'est pas formellement identifié;
- que la matrice de responsabilités de type RASCI n'est pas formellement approuvée;
- que certaines fonctions ne sont pas encore documentées ou manquent d'un approbateur.

Le manque d'identification formelle d'un propriétaire ainsi que des lacunes dans la documentation de la matrice de responsabilités de type RASCI pourraient causer des dysfonctionnements comme :

- une absence de prise de responsabilité sur les décisions reliées à la GIA;
- des tâches non exécutées, des omissions et des actions inégales quant à la gestion de la GIA.

3.1.1.D. Recommandation

Nous recommandons à la Division solutions numériques du Service des technologies de l'information d'officialiser le propriétaire de la GIA Citoyens.

3.1.1.E. Recommandation

Nous recommandons à la Division solutions numériques du Service des technologies de l'information de compléter, approuver et diffuser les rôles et les responsabilités pour la GIA Citoyens.

3.1.2. Encadrements de la Gestion centralisée des identités et des accès

La publication de politiques et de directives permet d'encadrer certains processus afin de limiter les risques d'inconsistances dans les actions posées et prévenir des contournements d'accès et des abus de privilèges. Typiquement, la GIA doit expliquer les principes de base et comprendre les éléments suivants :

- La gestion centralisée des identités : dès leur création jusqu'à leur désactivation ou résiliation;
- La gestion centralisée des accès : pour l'authentification et la gestion des accès aux actifs informationnels (octroi, modification, surveillance, retrait et révision périodique).

GIA Employés

La directive et le standard sur la gestion des accès logiques sont publiés sur l'intranet de la Ville. Il est à noter que ces encadrements concernent la gestion des accès dans son ensemble et ciblent toutes les identités et les actifs gérés par la Ville. Ces documents sont à jour, complets et formellement approuvés. De plus, la directive a été communiquée à l'ensemble des employés.

Pour ce qui est des encadrements plus spécifiques au cycle de vie des comptes de la GIA, nous avons examiné les processus suivants :

- Processus et procédures d'arrivée, d'interruption ou de départ d'un employé;
- Octroi et le retrait de comptes privilégiés;
- Gestion des accès des consultants;
- Principes directeurs pour la gestion de contrats qui mentionne certaines tâches reliées à la gestion des accès;
- Recueil de guides et d'instructions provenant de la base de connaissances des agents du Centre de services TI pour la GIA.

Nous notons que les processus et les procédures énumérés précédemment ne correspondent pas à une GIA.

Nous avons aussi constaté l'absence de procédures pour les points suivants :

- La gestion des accès propres à la GIA Employés, en conformité aux encadrements;
- La révision périodique des accès;
- La gestion du cycle de vie de comptes de tierces parties (fournisseurs, partenaires, consultants, bénévoles, etc.);
- La gestion du cycle de vie de comptes reliés aux actifs informationnels sous forme matérielle (serveurs, imprimantes, postes de travail, etc.) ou logicielle (bases de données, applications logicielles, sites web, etc.).

Étant donné que le projet de GIA est en cours, les processus et les procédures reliés à la GIA ne sont pas encore documentés.

L'absence de processus et de procédures pour la GIA engendrerait des risques de non-uniformité des façons de faire en matière de GIA, ainsi que de non-respect des rôles et responsabilités des parties prenantes lors de l'accès aux actifs informationnels de la Ville. Cela pourrait causer des accès non autorisés à des données sensibles.

3.1.2.A. Recommandation

Nous recommandons à la Direction sécurité de l'information du Service des technologies de l'information de documenter les processus et procédures propres à la Gestion centralisée des identités et des accès et de s'assurer de leur diffusion auprès des parties prenantes.

GIA Citoyens

La gestion des identités des citoyens se fait par l'entremise de la plateforme Dossier citoyen intégré (DCI). Celle-ci comporte deux volets :

- Mon Compte pour les citoyens;
- Mon Compte – vue employés, permettant aux employés de traiter les demandes en ligne des citoyens.

- ***Volet citoyens***

Une politique de confidentialité et des conditions d'utilisation du compte sont accessibles à partir du portail de la Ville. Elle est aussi accessible lors de la création d'un compte citoyen ou lors du changement de mot de passe. Nous avons répertorié les procédures suivantes sur le portail pour les citoyens :

- La création du compte;
- La modification de comptes citoyens et des entreprises;
- La suppression de comptes à la demande du citoyen.

Ces documents sont à jour, complets, formellement approuvés et dûment publiés.

Par contre, nous avons constaté :

- qu'il n'y a pas de procédure pour la révision périodique des comptes;
- que la procédure déclenchée par la demande de suppression d'un compte citoyen est manuelle et n'est pas documentée.

- ***Volet employés***

Un employé peut administrer des comptes de citoyens à partir d'une vue aux citoyens. Le Service de concertation des arrondissements a mis en place un site web à cet effet. Celui-ci fournit l'accès aux procédures, aux guides et formations pour la gestion de fonctionnalités concernant les comptes de citoyens et ses services afférents. Cependant, lors des entrevues, nous avons confirmé que les retraits des accès aux employés ne sont pas exécutés systématiquement et dépendent de chaque unité d'affaires.

L'absence de procédures pour la révision périodique des comptes et leur suppression pourrait engendrer des façons non uniformisées lors de l'exécution de ces tâches. Cela pourrait faire en sorte de laisser des accès indus aux données sensibles à certains utilisateurs.

3.1.2.B. Recommandation

Nous recommandons à la Division solutions numériques du Service des technologies de l'information de formaliser les encadrements pour la révision périodique et la suppression des comptes de la GIA Citoyens et de s'assurer de sa diffusion auprès des parties prenantes.

3.1.3. Stratégie de la Gestion centralisée des identités et des accès

Lors de la planification et l'implantation d'une GIA, il est primordial d'établir une stratégie globale qui implique toutes les parties prenantes. Parmi les étapes d'une bonne stratégie, nous retrouvons les éléments suivants :

- La portée du projet;
- Les besoins d'affaires;
- Les vigies;
- Les standards ou les meilleures pratiques adoptées;
- Les architectures actuelles et cibles.

GIA Employés

- ***Situation actuelle du projet***

Le projet de la GIA Employés a été initié en 2016, mais a subi des impacts en raison de départs d'employés clés, tels les architectes d'entreprise et de solutions de sécurité ainsi que le chef de livraison. Ces changements ont causé des enjeux sur la continuité du projet et l'harmonisation de travaux. De plus, l'initiative de création de comités, avec la participation des unités d'affaires, a été abandonnée.

Ainsi, le projet actuel est axé sur les technologies, c'est pourquoi il a priorisé :

- l'exécution des vigies technologiques;
- la livraison des outils pour rehausser l'authentification;
- le déploiement des infrastructures dans tous les environnements pour les outils choisis;
- la documentation des architectures et des matrices de responsabilités de type RASCI par outil.

Les éléments suivants ont été mis en exploitation :

- Le deuxième facteur d'authentification;
- L'intégration de l'authentification unique aux applications. Cela permet aux utilisateurs d'accéder à plusieurs applications en ne procédant qu'à une seule authentification;
- Le rehaussement de la complexité des mots de passe.

Cependant, le manque de documentation détaillée des architectures (actuelle et cible), des technologies en place, des besoins et des risques ont causé des enjeux importants, comme :

- la détection tardive de l'incompatibilité de l'ancien annuaire avec le nouvel annuaire;
- les coûts élevés de soutien de l'outil d'authentification ne permettant pas sa mise à jour à la dernière version;
- l'abandon de l'outil choisi pour la gestion et la gouvernance centralisées des identités;
- le besoin de réévaluation de l'outil des comptes à hauts privilèges, ayant des enjeux de soutien et de fonctionnalités.

Étant donné cette situation, le projet est tombé en mode urgence. L'équipe travaille pour redresser la situation et revoit la stratégie de la GIA.

- ***Portée du projet***

Pour ce critère, l'équipe de projet nous a fourni des documents dont :

- la feuille de route du programme de sécurité et de continuité TI (approuvée en 2018), dont la portée considère :
  - toutes les personnes (employés et externes) à l'exception des citoyens;
  - tous les actifs physiques représentant un point d'accès (p. ex. les serveurs, les imprimantes, les postes de travail);
  - tous les actifs logiques (p. ex. les bases de données, les applications, les services web);
- la charte du projet gestion des identités (approuvée en 2020) présente des différences entre certaines sections du document quant aux types d'utilisateurs. Par exemple, dans les objectifs, l'ensemble des utilisateurs et les systèmes connectés sont précisés alors que dans le tableau des utilisateurs finaux, on y retrouve uniquement les élus, les employés, les stagiaires et les consultants externes.

Nous avons observé que la portée initiale concernant la population desservie a changé en 2020 et qu'elle est maintenant ambiguë et n'identifie pas formellement toutes les identités gérées par la Ville (p. ex. les partenaires d'affaires, les fournisseurs, les actifs physiques et logiques).

Quant aux livrables, la nouvelle charte de projet précise les éléments requis pour la nouvelle solution (dont les documents d'architecture, les solutions technologiques, les processus visés, etc.). Cependant, nous avons relevé l'absence :

- de documentation des besoins d'affaires;
- de documentation des cas d'usage qui mettent en évidence les relations fonctionnelles entre les acteurs et la GIA;
- d'analyse détaillée des processus et des technologies déjà implantées;
- des enjeux et les contraintes à considérer par le projet.

- ***Stratégie globale et besoins d'affaires***

Engagement organisationnel

La GIA est un processus qui nécessite l'appui de la haute direction et l'engagement des différentes unités d'affaires. La directive pour la gestion des accès logiques mentionne que l'adoption d'une approche globale pour la gestion des accès est sous la responsabilité du CSI. Donc, ce dernier devrait avoir une implication formelle et régulière sur le projet de la GIA. Cependant, nous avons constaté que la seule rencontre avec ce comité à propos de la gestion des accès a été effectuée en janvier 2020. Le compte rendu montre qu'il y a eu des discussions concernant la nouvelle directive sur la gestion des accès logiques. Par contre, les rôles et les responsabilités du CSI sur la gestion des accès n'ont pas été présentés.

Phases du projet

À la revue de la feuille de route du projet GIA, qui détaille les principales phases d'implantation, nous avons observé :

- que les manquements mentionnés dans la charte du projet (section portée du projet) sont aussi reflétés dans la feuille de route;
- que les activités concernant les processus sont reliées à des outils et qu'il n'y a pas d'activité pour les processus de la GIA dans son ensemble;
- une absence de suivi des activités s'y rattachant (état d'avancement et tâches déjà achevées);
- un manque d'harmonisation entre les activités de chaque phase du projet. Par exemple :
  - les activités reliées à « l'outil d'accès GA » ne sont pas complétées;
  - concernant l'outil des comptes à hauts privilèges, la mise en production précède la documentation des processus.

Ces lacunes ne permettent pas de répondre intégralement à la portée du projet et aux besoins des utilisateurs.

- ***Vigies***

Une première vigie de solutions technologiques pour la GIA a été réalisée en 2016 et mise à jour en 2020. Elles évaluaient la conformité de plusieurs produits aux fonctionnalités inventoriées. Dans ces vigies, l'outil d'authentification et de gestion des accès choisi et implanté ne répondait que partiellement aux besoins de la Ville.

Finalement, en 2021, le STI a réalisé une nouvelle vigie qui ne prend en compte que les fonctionnalités de l'outil choisi.

Donc, l'équipe risquerait de choisir à nouveau une solution ne répondant pas à toutes les fonctionnalités identifiées dans l'ancienne vigie, ce qui mènerait à des lacunes vis-à-vis les objectifs du projet GIA.

- ***Standards et meilleures pratiques adoptés***

Le document « Contexte et impacts de la GIA » fait un recensement des lois et des encadrements à respecter. Les documents d'architecture de l'annuaire et de l'outil pour la gestion de l'authentification pour la gestion des accès font également la mention des directives, des guides et des normes internes de la Ville.

Cependant, ces documents ne font pas mention des normes ou des meilleures pratiques en matière de GIA tels le *National Institute of Standards and Technology (NIST)* ou le Cadre de gestion des identités pancanadien du Conseil canadien de l'identification et de l'authentification numériques (CCIAN) (ou le Conseil d'identification et d'authentification numérique du Canada)[2]. Ces normes

[2] Le Comité d'experts du Cadre de confiance (TFEC) du Conseil canadien de l'identification et de l'authentification numériques (CCIAN) développe le Cadre de confiance pancanadienMC depuis 2016.

établissent des mécanismes de contrôle et des exigences de sécurité, propres à la GIA, en fonction du degré de sécurité et de sensibilité des actifs à accéder. Cela permettrait à la Ville d'implanter des infrastructures et des processus de GIA normalisés assurant la protection adéquate de ses actifs informationnels.

- ***Architectures actuelles et cibles***

Il n'y a pas de document sur l'architecture de la GIA (actuelle et cible) qui la présente dans son ensemble incluant les identités, les services et leurs interactions. Les documents d'architecture fournis sont propres à chaque outil technologique et présentent seulement les composantes avec lesquelles chaque solution interagit.

En conclusion, les lacunes liées à la stratégie de la GIA à la Ville auraient un impact significatif sur la GIA. Cette gestion pourrait être non uniforme et non sécuritaire et priverait les utilisateurs d'une expérience unique et simplifiée des accès aux actifs informationnels. Ces manquements entraîneraient des besoins non comblés, des processus et procédures incomplets et des outils n'ayant pas les fonctionnalités requises. De plus, le manque d'information et d'interaction avec le CSI impliquerait un manque :

- d'adoption d'une approche transversale de gestion des accès commune aux unités d'affaires;
- de gestion de risques adéquate liée à la gestion des accès logiques;
- de collaboration des différentes parties prenantes pour la mise en œuvre efficace des bonnes pratiques de gestion des accès.

3.1.3.A. Recommandation

Nous recommandons à la Direction sécurité de l'information du Service des technologies de l'information pour la GIA Employés de préciser la portée du projet en s'assurant que les éléments suivants y figurent :

- Types d'utilisateurs;
- Tous les livrables reliés à la situation actuelle et cible (encadrements, processus et technologies).

3.1.3.B. Recommandation

Nous recommandons à la Direction sécurité de l'information du Service des technologies de l'information pour la GIA Employés de s'assurer que le Comité de sécurité de l'information connaît et adopte ses responsabilités telles que décrites dans la Directive de gestion des accès logiques.

3.1.3.C. Recommandation

Nous recommandons à la Direction sécurité de l'information du Service des technologies de l'information pour la GIA Employés de s'assurer de l'harmonisation des étapes dans chaque phase du projet de la Gestion centralisée des identités et des accès.

3.1.3.D. Recommandation

Nous recommandons à la Direction sécurité de l'information du Service des technologies de l'information pour la GIA Employés d'intégrer dans la stratégie du projet les éléments suivants :

- L'analyse du contexte technologique et des processus actuels;
- Les besoins d'affaires et les cas d'usage des différentes unités d'affaires.

3.1.3.E. Recommandation

Nous recommandons à la Direction sécurité de l'information du Service des technologies de l'information pour la GIA Employés d'intégrer dans les vigies les besoins d'affaires et les fonctionnalités identifiées.

3.1.3.F. Recommandation

Nous recommandons à la Direction sécurité de l'information du Service des technologies de l'information pour la GIA Employés de préciser formellement les meilleures pratiques adoptées dans le cadre du projet de la Gestion centralisée des identités et des accès.

3.1.3.G. Recommandation

Nous recommandons à la Direction sécurité de l'information du Service des technologies de l'information pour la GIA Employés d'établir l'architecture actuelle et cible pour l'ensemble du processus de la Gestion centralisée des identités et des accès.

GIA Citoyens

- ***Portée du projet***

Le projet appelé DCI répond aux besoins de citoyens et intègre leur identité numérique. Sa portée établit des mécanismes pour gérer les identités et les accès des citoyens en fonction de services demandés. Ces identités considèrent aussi le lien avec des entreprises. L'équipe du projet envisage aussi de couvrir les besoins des citoyens en tant que groupe familial (p. ex. les parents et les enfants).

Quant à l'implantation de l'outil pour l'authentification, sa portée fonctionnelle est définie adéquatement dans le document d'architecture avec des cas d'usage.

- ***Stratégie globale et besoins d'affaires***

Nous avons constaté que l'architecture du dossier citoyen a une vue globale, qui permet de voir la situation actuelle. Celle-ci présente une vue à haut niveau des interactions des citoyens avec les systèmes leur offrant des services.

Quant à l'architecture cible, elle présente les étapes à suivre et les priorités d'intégration des services au portail du dossier citoyen en fonction de la population desservie.

- ***Vigies***

La solution pour la gestion des identités des citoyens est la même que celle des employés. Il n'y a pas de vigie propre à la GIA Citoyens.

- ***Standards et meilleures pratiques adoptés***

Le projet a adopté le Cadre de confiance pancanadien (CCIAN) pour établir les niveaux d'assurance requis lors de l'identification d'un citoyen. Cependant, les travaux sont encore en cours.

De plus, lors de l'intégration des applications à l'authentification unique offerte par la GIA Citoyens, l'équipe du projet a adopté une norme internationale[3] reconnue dans le marché. Cette dernière autorise les applications à vérifier l'identité d'un utilisateur final en se basant sur l'authentification fournie par la GIA Citoyens, et ce, en suivant un processus simplifié et normalisé.

- ***Architecture actuelle et cible***

Parmi les documents audités, l'architecture actuelle et l'architecture cible de la GIA sont documentées de manière appropriée. De plus, les aspects techniques sont dûment formalisés, ce qui permet une meilleure compréhension de la solution implantée.

Nous considérons que les différents documents reliés à la stratégie de la GIA Citoyens sont adéquats.

Aucune recommandation n'est nécessaire.

---

[3] OIDC : *OpenID Connect* est un standard géré par l'organisme *OpenID Foundation*. C'est une simple couche d'authentification qui vérifie l'identité des utilisateurs.

3.1.4. Analyse de risques

Une analyse de risques pour la GIA établit les exigences et les contrôles à implanter afin de protéger les identités des utilisateurs et les accès aux actifs de la Ville. Ces contrôles répondent au degré de confidentialité, d'intégrité et de disponibilité de l'information à accéder.

Des niveaux d'assurance sont établis afin de définir les exigences de sécurité minimales requises pour l'identification des utilisateurs, l'authentification et l'intégration des nouvelles applications. Ils sont établis en conformité avec le degré de risque des informations à accéder. Par exemple, pour l'identification d'un utilisateur, le premier niveau n'exigerait aucune preuve d'identité physique. Pour le niveau le plus élevé, l'utilisateur doit se présenter physiquement et fournir des documents valides afin de prouver son identité.

GIA Employés

Nous avons audité l'analyse de risques et son plan d'action et nous avons relevé l'absence :

- d'adoption formelle de standards pour la sécurité de la GIA;
- d'adoption formelle d'un modèle de niveaux d'assurance pour l'identification, l'authentification et l'intégration des applications;
- de mesures de mitigation reliées aux technologies centralisées pour la GIA (p. ex. la gestion centralisée des accès par profil);
- d'information concernant le risque résiduel des scénarios, après l'implantation des mesures proposées;
- d'échéanciers avec des responsables attitrés.

En l'absence d'une analyse de risques adéquate, les mécanismes de contrôle implantés pourraient ne pas être adaptés au niveau de risque des actifs informationnels. Cela impliquerait que des risques TI importants ne seraient pas mitigés adéquatement (p. ex. la compromission des informations confidentielles et renseignements personnels).

3.1.4.A. Recommandation

Nous recommandons à la Direction sécurité de l'information du Service des technologies de l'information pour la GIA Employés d'établir formellement des niveaux d'assurance pour l'identification, l'authentification des utilisateurs ainsi que pour l'intégration des applications à la Gestion centralisée des identités et des accès.

3.1.4.B. Recommandation

Nous recommandons à la Direction sécurité de l'information du Service des technologies de l'information pour la GIA Employés de veiller à ce que l'analyse de risques propose des mesures de mitigation en fonction des technologies du projet de Gestion centralisée des identités et des accès ainsi que des standards adoptés par la Ville.

3.1.4.C. Recommandation

Nous recommandons à la Direction sécurité de l'information du Service des technologies de l'information pour la GIA Employés de s'assurer que les mesures de mitigation implantées sont conformes aux niveaux d'assurance établis pour l'identification, l'authentification des utilisateurs ainsi que pour l'intégration des applications à la Gestion centralisée des identités et des accès.

3.1.4.D. Recommandation

Nous recommandons à la Direction sécurité de l'information du Service des technologies de l'information pour la GIA Employés de s'assurer que le plan d'action permet le suivi de l'implantation des mesures de mitigation proposées.

GIA Citoyens

Nous avons obtenu un document énumérant les principaux risques de sécurité avec une liste de mesures de mitigation génériques qui font partie des bonnes pratiques de sécurité du marché, mais qui ne sont pas formellement reliées aux contrôles implantés dans le projet GIA Citoyens. De plus, lorsque nous analysons ce document, nous notons l'absence :

- d'impact de ces risques et leur probabilité de matérialisation;
- d'état d'implantation des mesures de mitigation proposées;
- d'un plan d'action concernant les mesures de mitigation à implanter, avec des dates et des responsables.

L'équipe de projet a réalisé une cartographie des renseignements personnels reliés au dossier citoyen. De ce travail, des recommandations en découlent. Cependant, la plupart des recommandations n'ont pas encore de date attendue de résolution.

Le STI nous a mentionné que les analyses d'impacts et de risques n'ont pas encore été réalisées en raison d'un manque de ressources. Cependant, l'équipe a amorcé des travaux pour l'implantation de contrôles de sécurité.

La GIA Citoyens a adopté le Cadre de confiance pancanadien (CCIAN) pour établir les niveaux d'assurance requis lors de l'identification de citoyens pour l'accès aux services. Ce standard est en cours d'implantation. L'équipe de la GIA Citoyens envisage de s'aligner avec une identité pancanadienne, mais ce projet est en cours d'analyse.

En l'absence d'une analyse de risques adéquate, les mécanismes de contrôle implantés pourraient ne pas être adaptés au niveau de risque des actifs informationnels. Cela impliquerait que des risques TI ne soient pas mitigés adéquatement (p. ex. la compromission des informations confidentielles).

3.1.4.E. Recommandation

Nous recommandons à la Division solutions numériques du Service des technologies de l'information pour la GIA Citoyens de réaliser une analyse de risques et d'impacts.

3.1.4.F. Recommandation

Nous recommandons à la Division solutions numériques du Service des technologies de l'information pour la GIA Citoyens de formaliser les niveaux d'assurance pour l'identification, l'authentification des utilisateurs ainsi que pour l'intégration des applications à la Gestion centralisée des identités et des accès.

3.1.4.G. Recommandation

Nous recommandons à la Division solutions numériques du Service des technologies de l'information pour la GIA Citoyens de s'assurer que les mesures de mitigation implantées sont conformes au niveau d'assurance établi pour l'identification, l'authentification des utilisateurs ainsi que pour l'intégration des applications à la Gestion centralisée des identités et des accès.

3.1.4.H. Recommandation

Nous recommandons à la Division solutions numériques du Service des technologies de l'information pour la GIA Citoyens de réaliser un plan d'action pour le suivi des mesures de mitigation proposées.

3.2. Gestion des utilisateurs (identités)

La gestion centralisée des utilisateurs permet de gérer les comptes et les rôles des identités dès leur création jusqu'à leur désactivation. Cela comprend aussi les comptes à hauts privilèges qui nécessitent des mécanismes plus robustes afin de les protéger contre des actes illicites.

GIA Employés

D'après les informations recueillies, la gestion des utilisateurs est décentralisée et ne constitue pas une GIA à proprement parler puisque :

- la gestion des utilisateurs actuelle (création, révision, retrait, modification, désactivation) obéit plutôt à des processus administratifs provenant de différentes unités d'affaires;
- les principales composantes de la GIA ne sont pas intégrées à un outil de gestion unique et ces processus ne sont pas centralisés;
- les critères et les exigences pour la création, la révision, le retrait, la modification et la désactivation de différents types de comptes ne sont pas harmonisés. À titre d'exemple :
  - pour créer des comptes des utilisateurs externes, il suffit d'avoir leur nom et leur compte courriel. Ainsi, s'il n'y a pas de date de fin de contrat, une durée de vie de deux ans est fixée par défaut;
  - la création de comptes d'employés suit un processus, formalisé par le SRH, qui assure la vérification de l'identité de nouveaux employés et laisse une trace dans le système. Lors du départ de l'employé, son compte est désactivé par un automatisme.

De plus, l'équipe du projet :

- envisage l'implantation d'un nouvel annuaire pour remplacer l'ancien annuaire, encore en production;
- remplacera l'outil pour la gouvernance et la gestion de profils qui avait été choisi au début du projet;
- a récemment implanté une voûte de mots de passe pour la gestion des comptes à hauts privilèges qui est en réévaluation.

Nous n'émettrons pas une nouvelle recommandation puisque les recommandations à la section 3.1.4. couvrent déjà les éléments à améliorer et les outils en place pour la gestion des identités seront tous remplacés éventuellement.

GIA Citoyens

- ***Volet citoyens***

Pour le cycle de vie des identités des citoyens, les mécanismes centralisés sont adéquats et normalisés pour les aspects suivants :

- L'inscription et la vérification des identités des utilisateurs;
- La désinscription de comptes (à la demande du citoyen);
- La désactivation de comptes (temporaire à la suite de tentatives infructueuses de connexion).

Par contre, nous n'avons pas trouvé de mécanisme permettant la désactivation des comptes inactifs. Ainsi, un compte citoyen n'est effacé qu'à sa demande et obéit à un processus manuel.

Le seul compte à haut privilège est géré par l'administrateur de la GIA Citoyens, qui est un employé. L'équipe envisage l'adoption de la solution des comptes à hauts privilèges prévue dans le GIA Employés pour cet administrateur. Les comptes de citoyens n'ont pas de droits à hauts privilèges. Les comptes utilisés pour les applications ont aussi des accès restreints.

Dans le cas d'une gestion inappropriée du cycle de vie des comptes, des incidents de perte, de vol, de compromission ou de falsification des identifiants pourraient se concrétiser.

3.2.A. Recommandation

Nous recommandons à la Division solutions numériques du Service des technologies de l'information d'implanter des mécanismes dans la GIA Citoyens pour la désactivation et la suppression de comptes citoyens inactifs.

3.3. Gestion de l'authentification

La GIA permet d'harmoniser les méthodes d'authentification et de réduire la multitude de mots de passe requis pour l'accès aux systèmes. Ceci simplifie la vie aux utilisateurs et réduit les risques des accès non autorisés. De plus, elle fournit des méthodes d'authentification normalisées et adaptées aux risques des informations à accéder. Par exemple, les paramètres d'authentification de mots de passe doivent être alignés avec la politique de la Ville (p. ex. la longueur minimale du mot de passe, l'inclusion de majuscules et de caractères spéciaux, l'impossibilité de réutiliser les précédents mots de passe). De plus, l'octroi des accès aux actifs de nature critique requiert l'implantation de plusieurs facteurs d'authentification (p. ex. ce qu'un utilisateur connaît (secret) et ce qu'il possède (un téléphone, une carte d'accès physique, etc.)).

Afin de détecter des tentatives d'accès non autorisées, chaque organisation doit disposer d'un processus de surveillance des accès. Cette surveillance permettra également une analyse plus efficace en cas d'incident de cette nature.

GIA Employés

L'outil GIA en place a intégré l'authentification à deux facteurs avec une solution reconnue dans l'industrie. Des efforts ont aussi été mis sur le rehaussement de la complexité des mots de passe. Comme nous l'avons mentionné dans la section 3.1.4. du rapport, l'analyse de risques et les niveaux d'assurances ne sont pas complétés. Ainsi, les méthodes d'authentification en place ne sont pas liées au niveau de risque des actifs à accéder.

Quant à la journalisation et la surveillance, les journaux des accès sont présents, mais des travaux sont en cours pour leur intégration à l'outil centralisé de gestion de journaux.

Nous n'émettrons pas une nouvelle recommandation puisque les recommandations à la section 3.1.4. couvrent déjà les éléments à améliorer. De plus, l'outil utilisé pour l'authentification sera remplacé.

GIA Citoyens

- ***Volet citoyens***

Une méthode d'authentification a été implantée afin de simplifier l'accès des citoyens. Seulement le mot de passe est utilisé avec un numéro de téléphone cellulaire et un courriel pour valider le compte d'un citoyen. Il n'y a pas d'authentification multifacteur. Par contre, il y a certains mécanismes qui réduisent les risques de leur compromission, dont la désactivation temporaire de comptes après un nombre déterminé d'échecs.

Comme indiqué dans la section 3.1.4. du rapport, l'analyse de risques et les niveaux d'assurances ne sont pas complétés. L'authentification n'est pas adaptée aux différents niveaux de risques. Présentement, certains paramètres dans les méthodes d'authentification ne sont pas en conformité avec le Standard de gestion des accès logiques de la Ville, dont la complexité des mots de passe.

- ***Volet employés***

Les employés accédant à la GIA Citoyens utilisent l'authentification de la GIA Employés. Par conséquent, la gestion de l'authentification des employés qui accèdent à la GIA Citoyens est gérée par la GIA Employés.

Pour la journalisation et la surveillance des accès, des journaux sont sauvegardés dans les infrastructures du DCI et aussi envoyés à l'outil centralisé de gestion de journaux. Ils sont dûment structurés et permettent l'exécution de recherches pour résoudre des incidents.

3.4. Gestion des accès

La GIA fournit des mécanismes pour l'approbation, l'octroi, la modification, le retrait et la révision des accès. Ceci favorise la conformité aux meilleures pratiques de sécurité comme le moindre privilège et le besoin de savoir. Dans ce contexte, les attributions de comptes à hauts privilèges doivent aussi être réglementées et suivies de plus près.

Avec la GIA, la révision périodique des droits d'accès pour la détection des changements d'affectation des utilisateurs est aussi simplifiée.

GIA Employés

D'après les informations recueillies, la gestion des accès est décentralisée et n'est pas organisée autour d'un outil central et ne constitue donc pas une GIA à proprement parler.

Selon la feuille de route, l'outil de gestion des accès n'est pas encore choisi. Il n'y a pas de mécanisme automatisé pour l'intégration de règles concernant la ségrégation de tâches, le moindre privilège et les autorisations incompatibles.

De plus, lors des rencontres avec les parties prenantes, elles nous ont confirmé que la gestion des accès est sous la responsabilité de chaque unité d'affaires et repose sur des processus administratifs.

Finalement, il y a absence de mécanismes centralisés et harmonisés permettant la révision périodique des accès.

Nous n'émettrons pas une nouvelle recommandation puisque les recommandations à la section 3.1.4. couvrent déjà les éléments à améliorer et qu'il n'y a pas encore d'outil en place.

GIA Citoyens

- ***Volet citoyens***

Le système fournit un accès de base aux citoyens et, au fur et à mesure qu'ils demandent des services, des accès à la carte leur sont octroyés. Par conséquent, la gestion des accès respecte, par défaut, les critères du besoin de savoir et du moindre privilège.

- ***Volet employés***

Lorsqu'un employé effectue des opérations d'entretien et de soutien pour les services offerts aux citoyens, il accède à l'environnement du DCI. Pour obtenir ses accès, il fait une demande auprès du Service de concertation des arrondissements. Un formulaire est disponible à cet effet. Cela permet de faire des demandes d'accès et de retrait d'employés au DCI et ses services afférents. Cependant, la révision périodique et le retrait des accès dépendent de chaque unité d'affaires et ne sont pas réalisés systématiquement.

En l'absence de processus de révision périodique des accès, la Ville fait face à un risque accru d'accès inappropriés ou superflus à certains actifs informationnels, qui ne sont pas en ligne avec les responsabilités du poste occupé de l'employé.

3.4.A. Recommandation

Nous recommandons à la Division solutions numériques du Service des technologies de l'information d'implanter un processus de révision périodique des accès à la GIA Citoyens.

3.5. Intégration des applications dans la Gestion centralisée des identités et des accès

L'intégration de nouvelles applications à la GIA permet de réduire le nombre d'authentifiants des utilisateurs et simplifie l'intégration de l'authentification aux applications. Par l'entremise d'une procédure écrite et formalisée, l'intégration des applications sera réalisée de manière plus uniforme et harmonisée.

GIA Employés

Une procédure sommaire est disponible pour l'intégration des applications à la GIA. L'équipe de projet a déjà intégré environ 125 applications parmi lesquelles la plupart utilisent le deuxième facteur. Chaque intégration est réalisée avec l'accompagnement de l'équipe de sécurité. Cette procédure devra être adaptée à la nouvelle réalité du projet.

Nous n'émettrons pas une nouvelle recommandation puisque les recommandations à la section 3.1.4. couvrent déjà les éléments à améliorer.

GIA Citoyens

En examinant le processus d'intégration des applications à la GIA, celui-ci passe par deux équipes. La première gère le portail du DCI et la deuxième, les infrastructures supportant la GIA Citoyens. Nous avons observé lors de nos travaux d'audit que :

- le formulaire du DCI récemment implanté répond aux besoins opérationnels et à la vision de la GIA. Il comporte des requis fonctionnels pour assurer une intégration adéquate au portail du DCI. L'équipe de la Division solutions numériques gère ces demandes;
- l'intégration des applications à la GIA Citoyens répond à un processus automatisé et dûment autorisé par l'administrateur de la GIA.

L'équipe qui gère le DCI vise à ce que ce dernier soit la source maîtresse pour les accès des citoyens. Cependant, le formulaire d'intégration à la GIA Citoyens ne demande aucune information concernant l'intégration au DCI. Lors des rencontres, il a été confirmé que cette condition n'était pas systématiquement évaluée.

L'intégration des applications n'est pas adaptée aux différents niveaux de risques. Nous avons déjà signalé dans la section 3.1.4. du rapport que l'analyse de risques et les niveaux d'assurances ne sont pas complétés.

En raison de cette lacune d'intégration des applications, la Ville subirait les impacts suivants :

- Un manque d'harmonisation et de visibilité concernant tous les accès octroyés aux citoyens par le DCI;
- Une gestion des accès qui n'est plus complètement centralisée;
- Un manque de traçabilité des actions commises par les citoyens sur des applications branchées uniquement à la GIA Citoyens.

3.5.A. Recommandation

Nous recommandons à la Division solutions numériques du Service des technologies de l'information de s'assurer que les applications intégrées à la GIA Citoyens le sont aussi au Dossier citoyen intégré et que tout écart est formellement justifié.

4. Conclusion

La Ville de Montréal (la Ville) a déclenché deux projets pour répondre aux besoins de la Gestion centralisée des identités et des accès (GIA) des employés et des citoyens. Ce qui a mené à l'implantation de deux solutions distinctes, une pour les citoyens et une autre pour les employés.

La GIA Citoyens, dans son ensemble, ne présente pas de risque majeur de confidentialité, d'intégrité et de disponibilité des données. Les mécanismes de contrôle en place démontrent une saine gestion de la GIA. La stratégie est adéquate et considère autant la situation actuelle que la vision à long terme. Les accès octroyés aux citoyens répondent aux critères de moindre privilège et du besoin de savoir. 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. Ce qui permettrait d'intégrer des mécanismes de contrôle uniformisés et reconnus dans le marché pour la protection des renseignements personnels et la sécurité des services offerts aux citoyens.

Par contre, le projet de la GIA Employés étant en redémarrage, plusieurs critères n'ont pas pu être évalués. Nous avons concentré nos travaux d'audit sur la gouvernance du projet. Nous avons relevé des lacunes importantes telles que le manque d'implication régulière du Comité de sécurité de l'information (CSI), l'absence d'un propriétaire du processus et d'une stratégie globale. L'analyse de risques et les mesures de mitigation proposées ne répondent pas à une gestion des identités et des accès centralisée. Les contrôles en place inventoriés répondent plutôt à des mécanismes décentralisés et administratifs. Par conséquent, les outils et les processus en place ne permettent pas d'assurer une gestion de risque adéquate concernant la confidentialité, l'intégrité et la disponibilité des données de la GIA. Néanmoins, des efforts ont été mis pour l'intégration des applications à la GIA et pour le rehaussement de la sécurité de l'authentification. Cela a malgré tout permis aux utilisateurs de réduire leur nombre de mots de passe.

La Ville n'est pas encore dotée d'un outil qui permet la centralisation des identités et des accès des employés.

Plus précisément, voici les détails selon les critères d'évaluation :

Critère d'évaluation – Gouvernance

Concernant la GIA Citoyens :

Le propriétaire du processus de la GIA Citoyens n'est pas formellement identifié et les matrices des rôles et des responsabilités s'y rattachant ne sont pas finalisées ni formellement approuvées.

Les encadrements de la GIA Citoyens sont adéquats dans l'ensemble à l'exception d'encadrements pour la révision périodique des accès et la suppression des comptes, qui sont manquants.

La stratégie de la GIA Citoyens est adéquatement documentée et comprend les principaux éléments qui la composent :

- Portée du projet;
- Stratégie globale et besoins d'affaires;
- Standards et meilleures pratiques adoptés;
- Architectures actuelles et cibles.

L'analyse de risques n'évalue pas l'impact et la probabilité de matérialisation des scénarios des risques. De plus, il n'y a pas encore de plan d'action concernant les mesures de mitigation à implanter. Enfin, les niveaux d'assurance pour l'identification, l'authentification et l'intégration des applications à la GIA ne sont pas formellement établis.

Concernant la GIA Employés :

Le propriétaire du processus de la GIA à la Ville n'est pas formellement identifié et les matrices des rôles et des responsabilités s'y rattachant ne sont pas documentées.

Les encadrements et les processus propres à une GIA ne sont pas complétés ni formalisés.

La stratégie de GIA Employés présente des lacunes dans plusieurs aspects :

- La portée quant aux types d'utilisateurs n'est pas bien définie;
- Le CSI et les unités d'affaires ne sont pas impliqués régulièrement;
- Il y a absence d'harmonisation des phases et des livrables du projet;
- L'analyse du contexte actuel (processus et technologique) et les besoins d'affaires ne sont pas documentés;
- Les vigies n'ont pas intégré les besoins d'affaires et les fonctionnalités identifiées;
- Il n'y a pas d'adoption formelle de normes ou de meilleures pratiques pour la GIA;
- Il y a absence d'architectures actuelles et cibles.

L'analyse de risques n'est pas complète et les mesures de mitigation ne sont pas alignées à une GIA et à des normes du marché. De plus, les niveaux d'assurance pour l'identification, l'authentification et l'intégration des applications à la GIA ne sont pas formellement définis.

Étant donné que le projet est en redémarrage et que les outils actuels seront remplacés, nous n'avons pas fait une évaluation des autres critères initialement établis de la portée de cet audit. Cependant, nous avions émis des recommandations à la section 3.1.4. qui permettraient d'améliorer des éléments concernant les critères non évalués :

- Gestion des utilisateurs (identités);
- Gestion de l'authentification;
- Gestion des accès;
- Intégration des applications dans la GIA.

Critère d'évaluation – Gestion des utilisateurs (identités)

Les utilisateurs pour la GIA Citoyens sont gérés de façon adéquate mis à part l'absence d'un mécanisme pour la suppression de comptes.

Critère d'évaluation – Gestion de l'authentification

Nous avons constaté que la gestion de l'authentification de la GIA Citoyens n'est pas encore adaptée aux niveaux d'assurance qui établissent les exigences de sécurité en fonction du degré de confidentialité des informations à accéder.

Critère d'évaluation – Gestion des accès

La gestion des accès à la GIA Citoyens est adéquate. Par contre, pour les accès des employés au dossier des citoyens, la révision périodique et le retrait des accès dépendent de chaque unité d'affaires et ne sont pas réalisés systématiquement.

Critère d'évaluation – Intégration des applications dans la GIA

Le processus d'intégration des applications est adéquat dans son ensemble pour la GIA Citoyens, mais les équipes ne s'assurent pas systématiquement que les applications intégrées à la GIA Citoyens le sont aussi au Dossier citoyen intégré (DCI) et que tout écart est formellement justifié. De plus, l'intégration des applications doit s'adapter aux niveaux d'assurance établis à la section 3.1.4.

5. Annexe

5.1. Objectif et critères d'évaluation

Objectif

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

Critères d'évaluation

Critère 1 : Gouvernance
Il existe une gouvernance de la GIA adéquatement documentée qui comprend la définition des rôles et responsabilités, des politiques et des encadrements, une stratégie et une analyse de risques qui établit les exigences et contrôles à implanter.

Critère 2 : Gestion des utilisateurs (identités)
Des mécanismes sécuritaires pour la gestion des identités des utilisateurs et des comptes privilégiés sont en place. Ils couvrent le cycle de vie des utilisateurs, et ce, dès l'inscription jusqu'à la résiliation des comptes.

Critère 3 : Gestion de l'authentification
Des mécanismes d'authentification numérique, conformes aux meilleures pratiques de l'industrie, sont en place et répondent au niveau de risque des actifs informationnels à protéger.

Critère 4 : Gestion des accès
La gestion des accès est réalisée en se conformant aux meilleures pratiques de sécurité (p. ex. le principe du moindre privilège, la séparation des tâches, la révision périodique des accès).

Critère 5 : Intégration des applications dans la GIA
L'intégration des applications de la Ville et tierces parties aux fonctionnalités d'authentification de la GIA obéit à une procédure normalisée et formellement établie.