4.7.

Gestion des accès logiques (SIMON, PAIE, OASIS)

(Service des technologies de l'information, Service des finances et Service des ressources humaines)

Le 10 janvier 2020

Rapport annuel 2019
Bureau du vérificateur général
de la Ville de Montréal

OBJECTIF

S'assurer que les accès logiques aux applications financières SIMON, PAIE et OASIS sont correctement gérés et limitent les risques d'accès non autorisés ou non appropriés en plus de restreindre les risques de fraude ou de collusion.

RÉSULTATS

Le Service des technologies de l'information (STI), le Service des finances et le Service des ressources humaines gèrent adéquatement les accès logiques des applications financières sous leur responsabilité.

En effet, les applications financières SIMON, PAIE et OASIS disposent des mécanismes de contrôle appropriés suivants :

- Des profils d'accès préétablis en fonction du poste occupé où des contrôles compensatoires sont en place et permettent d'assurer que les accès accordés sont pertinents;
- Les paramètres fixés pour l'authentification et la gestion des applications sont adéquats compte tenu de la plateforme sur laquelle elles sont hébergées;
- Il existe une surveillance périodique des accès logiques;
- Les comptes à hauts privilèges sont légitimes et sont en nombre limité. Ceux des applications OASIS et PAIE sont surveillés;
- Les droits conflictuels existants sont restreints et autorisés.

Néanmoins, nous avons relevé les éléments suivants qui nécessiteraient des améliorations :

- À propos des utilisateurs cumulant les tâches incompatibles de création de bons de commande et de réception de biens et services, bien que les demandes de dérogation aient été dûment approuvées par leur gestionnaire, les unités d'affaires ne font pas de façon systématique de suivi a posteriori afin de surveiller ces opérations;
- Même si certains principes de la gestion des accès logiques sont connus et appliqués, ils ne sont pas inclus dans les encadrements;
- Il n'existe aucun mécanisme permettant de valider, a posteriori, la robustesse des mots de passe utilisés;
- La revue des accès à l'application OASIS pour les Bureaux Accès Montréal doit être effectuée de façon plus fréquente;
- Les comptes à hauts privilèges de SIMON ne sont pas surveillés adéquatement.

En marge de ces résultats, nous avons formulé différentes recommandations aux unités d'affaires.

Les détails de ces recommandations ainsi que notre conclusion sont décrits dans notre rapport d'audit présenté aux pages suivantes.

Soulignons que les unités d'affaires ont eu l'opportunité de formuler leurs commentaires, lesquels sont reproduits à la suite des recommandations de notre rapport d'audit.

TABLE DES MATIÈRES

LISTE DES SIGLES

ACF2	Logiciel de contrôle d'accès IBM
BAM	Bureaux Accès Montréal
CGI	contrôles généraux informatiques
GIA	Gestion des Identités et des Accès
SPVM	Service de police de la Ville de Montréal
STI	Service des technologies de l'information
TSO	Time Sharing Option (interpréteur de lignes de commande utilisé sur les grands systèmes IBM)

1. CONTEXTE

Les accès aux applications sont déterminés à l'aide d'un code d'usager et d'un mot de passe. Ces éléments constituent la clé d'accès qui permettra à son détenteur d'effectuer dans l'application les actions qui lui auront été octroyées.

L'activité d'attribution des permissions aux actions et aux données qu'un usager peut effectuer à l'intérieur d'une application constitue la gestion des accès logiques. Les bonnes pratiques édictent que :

- le mot de passe utilisé soit robuste;
- les codes d'accès à hauts privilèges[1] soient autorisés en nombre restreint;
- les accès d'un usager soient réévalués périodiquement;
- les accès d'un usager soient maintenus à un niveau suffisant et approprié;
- les accès d'un usager ne permettent pas l'accomplissement de tâches incompatibles.

Ces pratiques permettent de limiter en tout temps les risques d'accès non autorisés ou non appropriés et de minimiser les risques d'erreurs, de fraude ou de collusion.

Il existe principalement trois applications qui gèrent des informations financières de la Ville de Montréal (la Ville), soit :

- SIMON : système intégré de la Ville dont les principales fonctions sont la comptabilité et l'approvisionnement. Il comprend plus de 28 000 utilisateurs;
- PAIE : application qui gère la paie d'environ 23 000 employés. Le nombre d'utilisateurs se chiffre à plus de 280 (environ 1,9 G$ pour le budget de 2019);
- OASIS : système pour la recette des taxes municipales (environ 4,8 G$ pour l'année 2019). Cette application comporte plus de 400 utilisateurs.

Ces trois applications sont hébergées par la Ville.

Précisons également que dans le cadre de ses travaux d'audit annuels portant sur les contrôles généraux informatiques (CGI), des travaux en regard de la gestion des accès logiques sur ces applications financières sont conduits.

[1] Utilisés pour l'administration d'une application. Son utilisateur possède des droits illimités comme, entre autres, la lecture de toute information, la configuration de paramètres et même la modification et la destruction de données.

L'application SIMON est un système intégré de gestion comprenant notamment des modules de grand livre, d'approvisionnement et de paie pour les traitements de la rémunération des élus, des juges et des retraités ainsi que pour le Service de police de la Ville de Montréal (SPVM) depuis le 1er janvier 2019. La plateforme est une base de données Oracle.

Les applications PAIE et OASIS sont hébergées sur un ordinateur central (IBM) dont les accès sont gérés par le Logiciel de contrôle d'accès IBM (ACF2). L'accès à ces applications se fait sur deux niveaux : le premier représente l'accès à l'ordinateur central et le second à l'application même. Les environnements informatiques sont donc distincts que l'on parle des applications SIMON, PAIE ou OASIS.

Pour évaluer correctement la gestion des accès logiques de chacune des applications financières faisant l'objet de notre audit, il est important de comprendre la façon dont les demandes de création, de modification et de retrait d'accès sont gérées. De plus, il est important de connaître les diverses actions que les profils attribués peuvent exécuter dans l'application, ceci afin de déceler les droits d'accès qui sont le plus à risque. Finalement, nous devons connaître les profils d'accès incompatibles qui entraînent des risques d'enregistrement de transactions pouvant ouvrir la porte à de la fraude ou à de la collusion.

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 gestion des accès logiques aux applications financières SIMON, PAIE et OASIS. Nous avons réalisé cette mission conformément à la Norme canadienne de missions de certification (NCMC) 3001 du Manuel de CPA Canada – Certification ainsi qu'aux autres normes canadiennes de certification s'appliquant au secteur public émises par le Conseil des normes d'audit et de certification, soutenu par CPA Canada.

Le présent audit avait pour objectif de s'assurer que les accès logiques aux applications financières SIMON, PAIE et OASIS sont correctement gérés et limitent les risques d'accès non autorisés ou non appropriés, en plus de restreindre les risques de fraude ou de collusion.

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 les 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.

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.

L'objet de notre audit a porté uniquement sur la gestion des accès logiques. Afin de délimiter notre intervention, il fut décidé d'auditer les principales applications de nature financière, soit les suivantes :

- SIMON;
- PAIE;
- OASIS.

Dans ce contexte, les trois unités d'affaires suivantes furent rencontrées pour les applications ciblées :

1. le Service des technologies de l'information (STI) pour l'application SIMON;
2. le Service des finances pour l'application OASIS;
3. le Service des ressources humaines pour l'application PAIE.

De plus, aux fins de notre audit et afin de ne pas dupliquer les travaux, nous avons exclu de notre mission les tâches réalisées pour évaluer les contrôles généraux des technologies de l'information dans le cadre de l'audit des états financiers de la Ville. Ces travaux servent à s'assurer que les informations produites par les systèmes financiers fournissent une information exemptée d'anomalies significatives.

Notre audit a été réalisé d'avril 2018 à décembre 2019 et nos tests ont couvert les périodes de février 2018 à février 2019. 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'en janvier 2020.

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 chacune des unités d'affaires auditées. Par la suite, le rapport final a été transmis à la Direction générale, ainsi qu'à chacune des unités d'affaires concernées, pour l'obtention de plans d'action et d'échéanciers pour leur mise en œuvre.

3. RÉSULTATS DE L'AUDIT

3.1. Gouvernance

3.1.A. Contexte et constatations

La publication de politiques et de directives permet d'encadrer les diverses facettes d'un sujet et de limiter les risques d'inconsistances dans les actions posées en lien avec les divers éléments d'un processus.

Afin d'encadrer le processus de gestion des accès logiques (p. ex. l'octroi, la modification, le retrait et la révision), la Ville a émis des encadrements. Le respect de ceux-ci permet d'assurer l'autorisation des accès octroyés et des actions qui leur sont permises dans ces applications. Une revue périodique de ces droits d'accès permet d'assurer que le processus fonctionne adéquatement.

Nous avons examiné les divers encadrements de la Ville en regard de la gestion des accès logiques.

Nous avons relevé les politiques et les directives suivantes :

- la Politique de sécurité de l'information (émise en 2006);
- la Directive sur la gestion des accès aux ressources informationnelles (émise en 2006);
- le Standard sur les clés d'accès aux ressources informationnelles (émis en 2006).

Également, dans le cadre du projet Gestion des Identités et des Accès (GIA), une ébauche de directive portant sur la gestion des accès logiques nous a été remise. La GIA permet l'identification unique des usagers ayant besoin d'accéder aux ressources informationnelles ou aux ressources physiques (p. ex. le local, le téléphone, le matériel) de la Ville. Cette gestion permet alors de mieux gérer les impacts des événements (embauche, promotion, mutation, départ) sur les différents accès octroyés et ainsi renforcer la sécurité.

Notre premier constat révèle que certains paramètres de robustesse des mots de passe énoncés dans le Standard sur les clés d'accès aux ressources informationnelles sont faibles ou ne sont pas respectés. En effet, au-delà d'une longueur acceptable pour ce dernier, il n'y a aucune combinaison obligatoire de caractère qui y soit spécifiée. Également, même si ce standard précise que les mots de passe doivent expirer dans un délai de 30 jours, notre audit des systèmes examinés révèle plutôt la mise en place d'un délai de 90 jours.

De plus, l'examen du contenu des encadrements en vigueur révèle l'absence de certains principes, soit :

- Privilège minimal : les privilèges d'accès attribués sont restreints aux ressources informationnelles requises pour accomplir les tâches nécessaires;
- Privilège de séparation des tâches : les responsabilités liées à une activité de nature essentielle ou stratégique sont réparties entre plusieurs entités (p. ex. les personnes, les processus) afin d'éviter qu'une seule entité n'exerce un contrôle sur l'ensemble de l'activité;
- Principe de traçabilité : les accès et les tentatives d'accès aux actifs informationnels supportant les processus d'affaires critiques ou stratégiques sont enregistrés et conservés.

Ces principes, que l'on retrace toutefois à l'intérieur du projet GIA de la directive qui nous a été présentée, sont présentement appliqués de façon informelle.

Le manque d'encadrements, de politiques et de procédures pourrait engendrer des inconsistances dans le traitement et la gestion des accès logiques (p. ex. l'octroi d'accès non autorisés ou non justifiés).

Nous sommes d'avis que dans le cadre du projet GIA, le Standard sur les clés d'accès aux ressources informationnelles devrait être revu afin que soient établis les futurs paramètres relatifs à la robustesse et à la fréquence des modifications des mots de passe.

Également, nous croyons qu'il est pertinent de poursuivre les démarches d'adoption d'une directive portant sur la gestion des accès logiques qui contiendrait les principes énoncés précédemment.

Nous sommes toutefois conscients que la vétusté de certaines plateformes technologiques freine :

- l'uniformisation et la mise en place de paramètres plus rigoureux;
- la mise à jour des encadrements relatifs aux paramètres sur les mots de passe.

RECOMMANDATION

3.1.B. Nous recommandons au Service des technologies de l'information, dans le cadre du projet Gestion des Identités et des Accès, de :

- **mettre à jour ses encadrements relatifs à la gestion des accès logiques et plus particulièrement le Standard sur les clés d'accès aux ressources informationnelles afin que soient établis les futurs paramètres relatifs à la robustesse et à la fréquence des modifications des mots de passe;**
- **poursuivre ses démarches d'adoption d'une directive portant sur la gestion des accès logiques afin que les principes de privilège minimal, de séparation des tâches et de traçabilité soient clairement établis.**

RÉPONSE DE L'UNITÉ D'AFFAIRES

3.1.B. Service des technologies de l'information

Le standard de gestion des accès logiques est en cours d'élaboration et couvrira les critères de longueur, de complexité et de période de validité de mots de passe cohérents avec les bonnes pratiques de l'industrie.

La mise en place de ces bonnes pratiques est en cours dans le cadre du programme de sécurité. Cette initiative est en phase de réalisation et vise à être implantée en 2020.

La Directive sur la gestion des accès logiques a été soumise au Comité de sécurité de l'information et se trouve en révision par les membres du Comité. Celle-ci pourra ensuite être soumise pour approbation par le directeur général. ***(Échéancier prévu : décembre 2020)***

3.2. Octroi des accès

3.2.A. Contexte et constatations

Les accès consentis à une application doivent être appropriés en fonction des tâches à accomplir par les usagers. De plus, l'usager ne doit pas détenir des droits d'accès superflus par rapport à ses besoins.

Afin de s'assurer que les accès sont accordés en fonction des besoins et que le principe de privilège minimal est respecté dans les accès consentis aux applications faisant l'objet de notre audit, nous avons tenté de répondre aux questions suivantes :

- Les accès accordés sont-ils appropriés compte tenu des tâches de l'utilisateur ?
- L'usager détient-il plus de droits dans l'application que ce qui lui est nécessaire ?

Compte tenu de la complexité des accès consentis à certaines applications, l'utilisation de profils préétablis en fonction des tâches à accomplir pour des usagers modèles permet de mieux gérer ces accès et de minimiser les risques que ces derniers détiennent des droits superflus à leurs besoins.

Notre audit nous a permis de constater que pour les applications SIMON, PAIE et OASIS, les accès accordés sont appropriés, compte tenu des tâches de l'utilisateur. De plus, pour les applications PAIE et OASIS, des profils préétablis sont utilisés permettant ainsi de fixer l'octroi de ces accès. Pour l'application SIMON, un script génère quotidiennement un rapport permettant d'identifier les usagers pour lesquels un mouvement de poste est survenu. Faisant suite à ce rapport, un examen manuel des droits d'accès détenus doit être effectué et, s'il y a lieu, d'y apporter les corrections nécessaires. Nos tests ont confirmé que ces révisions étaient efficaces.

Aucune recommandation n'est nécessaire.

3.3. Authentification et gestion des mots de passe

3.3.A. Contexte et constatations

La clé d'accès à une application, soit la combinaison d'un code d'usager et d'un mot de passe, se doit d'être robuste et assez contraignante afin de limiter les risques d'accès non autorisés.

Nous avons examiné les paramètres des mots de passe qui ont été fixés pour chacune des trois applications faisant l'objet de notre audit. Nos travaux ont révélé que les paramètres fixés sont adéquats compte tenu des limitations technologiques des plateformes sur lesquelles ces applications sont hébergées. En effet, en raison de la vétusté des applications OASIS et PAIE, des modifications de paramètres nécessiteraient des efforts considérables tenant compte que ceux-ci pourraient être remplacés dans un avenir rapproché.

Mentionnons cependant qu'il n'existe aucun mécanisme d'identification, a posteriori, de la robustesse des mots de passe utilisés par l'ensemble des usagers de l'application au-delà des critères fixés par les paramètres. Ces mécanismes permettent de qualifier le mot de passe en fonction des meilleures pratiques, ainsi l'usager obtiendrait immédiatement un commentaire sur la sécurité de son mot de passe (p. ex. insuffisante, bonne, excellente), et celui-ci pourrait être examiné par la suite sur sa qualité de robustesse.

Bien qu'il ne soit pas efficient de développer de tels mécanismes sur d'anciennes plateformes, il serait pertinent d'envisager de mettre en place pour de futures applications sensibles, notamment dans le cadre de la GIA, des mécanismes d'identification de la robustesse des mots de passe utilisés par les usagers.

Des accès non autorisés pourraient survenir dans le cas où des usagers utiliseraient des mots de passe qui ne seraient pas suffisamment robustes. Néanmoins, l'usager malveillant n'a pas accès directement à l'application, il doit d'abord s'authentifier au réseau.

RECOMMANDATION

3.3.B. Nous recommandons au Service des technologies de l'information de développer et de mettre en place des mécanismes d'identification de la robustesse des mots de passe pour les futures applications appropriées.

RÉPONSE DE L'UNITÉ D'AFFAIRES

3.3.B. Service des technologies de l'information

Un document d'architecture détaillée sur les mécanismes à mettre en place pour la validation de la robustesse des mots de passe est en rédaction et fait partie des travaux qui seront implantés en 2020.

(Échéancier prévu : décembre 2020)

3.4. Surveillance et revue des accès

3.4.A. Contexte et constatations

Un processus d'attribution des accès est en place pour chacune des applications faisant l'objet de notre audit. Toutefois, il peut se produire plusieurs événements dans la carrière de son détenteur (p. ex. sa promotion, sa mutation, son départ). Il est alors essentiel qu'un mécanisme de révision récurrent des accès détenus soit en place et fonctionne correctement afin de retirer tout accès qui ne serait plus légitime.

À cet effet, nous avons examiné les processus de révision des accès pour chacune des applications de notre audit.

Application SIMON

Les accès à l'intérieur de cette application sont alloués par modules (p. ex. GL, Achats, Inventaire), par responsabilité (p. ex. faire une interrogation ou une transaction) et par niveau d'intervention (p. ex. global, unité administrative, montant).

Soulignons au départ que chaque employé possède un accès par défaut à l'application SIMON aux fins de postulation (le service de postulation en ligne), de même que pour consulter son dépôt électronique de paie (le service en ligne aux employés).

Il n'y a pas de validation périodique formelle auprès des gestionnaires. Toutefois, un script est lancé quotidiennement qui désactive les accès à la suite d'un mouvement de l'usager inscrit au registre des postes. Celui-ci compile tous les mouvements des employés durant leur carrière à la Ville.

De plus, ce script génère un rapport qui doit être examiné par les responsables du Centre d'expertise SIMON afin que soient appliquées les actions appropriées. D'autres scripts d'analyses sont également produits permettant de détecter des modifications dans les besoins d'accès à l'application SIMON.

Également, des routines effectuées par les administrateurs du système (sysadmin[2]) à une fréquence quotidienne, hebdomadaire ou mensuelle, selon le cas, permettent de faire ressortir des anomalies dans les droits accordés aux usagers et permettent de les corriger rapidement. Finalement, tout droit de poser une action précise dans un module (p. ex. responsabilité) et qui est non utilisé par l'usager pendant une période de six mois est automatiquement désactivé.

Nous avons validé divers rapports entre le 11 septembre 2018 et le 21 janvier 2019 et les actions correctives ont été posées.

Aucune recommandation n'est nécessaire.

Application PAIE

L'accès à l'application PAIE se fait sur deux niveaux. Le premier représente l'accès à l'ordinateur central IBM et le second à l'application PAIE en particulier. Les accès à cette application sont validés annuellement afin de s'assurer que les droits détenus sont encore appropriés ou pertinents. Les accès sont également validés de façon bimestrielle pour les départs. Cet exercice permet notamment de nettoyer la liste des usagers de l'application car, si l'usager ne se connecte pas à l'ordinateur central IBM (ACF2) à l'intérieur d'un délai de trois mois, son code d'accès IBM sera suspendu dans un premier temps puis détruit subséquemment après 13 mois d'inactivité. Le code d'accès à l'application PAIE sera toujours actif et présent dans la liste des utilisateurs de l'application même si cet accès est suspendu après six mois. La revue des accès mise en place permet l'épuration de ces codes d'accès.

Nous avons validé les rapports de novembre 2018 et notre audit nous a permis de constater que les procédures décrites sont effectuées.

Aucune recommandation n'est nécessaire.

[2] Un accès administrateur permet l'accès à toutes les fonctions et données d'une application. Il permet également d'effectuer la maintenance de celle-ci.

Application OASIS

De la même manière que l'application PAIE, l'accès à l'application OASIS se fait sur deux niveaux. L'accès à IBM est automatiquement suspendu et détruit ultimement si l'usager ne se connecte pas à l'intérieur des délais prescrits mentionnés précédemment.

Compte tenu du paramètre de destruction, l'usager n'aura plus accès à l'application OASIS bien que celui-ci soit toujours actif dans l'application. Bien qu'il soit important que les accès soient revus périodiquement, un effort doit être effectué dans ces circonstances afin de retirer les accès non justifiés dans la base de données de l'application.

Notre audit de l'application OASIS, dont le travail a porté sur la période de février 2018 à janvier 2019, nous a permis de constater qu'un suivi mensuel est effectué auprès des gestionnaires des usagers de l'application. Cependant, en ce qui a trait aux Bureaux Accès Montréal (BAM), cet exercice n'est effectué que deux fois par année. Un examen des codes d'accès inutilisés depuis plus d'un an est également effectué par le responsable de la sécurité de l'application OASIS.

Nous avons examiné les rapports de septembre 2018 à janvier 2019 portant sur les accès inutilisés depuis plus d'un an et les accès inutiles ont été retirés.

Malgré ce travail, nous sommes d'avis que la révision des accès pour les BAM gagnerait à être effectuée plus fréquemment, étant donné que la majorité des personnes qui y travaillent ont des accès relatifs aux encaissements de taxes.

Des accès non légitimes pourraient demeurer actifs advenant l'absence d'une surveillance et d'une revue régulières des accès consentis.

RECOMMANDATION

3.4.B. Nous recommandons au Service des finances d'effectuer une revue plus fréquente des accès octroyés aux personnes travaillant dans les Bureaux Accès Montréal à l'application OASIS.

RÉPONSE DE L'UNITÉ D'AFFAIRES

3.4.B. Service des finances

Les travaux de l'audit de l'application OASIS ont porté sur la période de février 2018 à janvier 2019.

La procédure a été revue à la suite de la réception des recommandations de l'audit. Deux importantes modifications ont été apportées au processus en lien avec les accès Bureaux Accès Montréal :

1. *La validation des accès auprès des arrondissements est maintenant effectuée tous les trimestres;*
2. *Le système Système de point de vente a été implanté dans tous les Bureaux Accès Montréal. Avec ce Système de point de vente, les seuls changements qu'ils peuvent faire sont des changements d'adresse. Ils n'ont pas accès aux autres données qu'en mode visualisation. Le risque d'accès soulevé par les travaux d'audit a été éliminé.*

Nous considérons cette recommandation réglée.

(Échéancier prévu : immédiat)

3.5. Comptes à hauts privilèges

3.5.A. Contexte et constatations

Habituellement, les usagers ne doivent posséder que les accès nécessaires à l'accomplissement de leurs tâches. Cependant, les applications comportent des codes d'accès dits à hauts privilèges, permettant d'effectuer des tâches particulières et qui ne peuvent être dévolues autrement que par des droits d'accès réguliers de l'application. Ce sont donc des accès très sensibles qui ont un grand impact sur les données.

Ces accès doivent être distribués en nombre limité et surveillés étroitement.

Chacune des applications ayant fait l'objet de notre audit possède ses propres codes d'accès à hauts privilèges.

Application SIMON

Notre audit nous a permis de constater que trois utilisateurs possèdent les droits d'administrateur système (sysadmin) dans l'application qui sont liés à leur code d'usager. De plus, ce sont les mêmes utilisateurs qui ont accès au compte générique sysadmin[3], ce qui est acceptable.

Nous avons également identifié les droits permettant d'octroyer les accès comme étant à hauts privilèges dans l'application. Notre audit a révélé que seulement les sysadmin de même que les personnes travaillant au Centre d'expertise SIMON possèdent ces droits, ce qui est adéquat.

Nous avons constaté que les transactions effectuées à l'aide du compte générique sysadmin ne font pas l'objet d'une journalisation[4] adéquate puisque celle-ci est manuelle. Dans le cadre des travaux annuels sur les CGI, les auditeurs ont d'ailleurs émis en 2015 la recommandation « Compte générique à hauts privilèges sur l'application SIMON » à cet effet et elle n'est toujours pas réglée.

Nos travaux nous permettent de conclure que les accès privilégiés de cette application sont adéquatement octroyés, mais non surveillés.

Mis à part la recommandation émise en 2015, aucune autre recommandation n'est nécessaire.

Application PAIE

Les accès à hauts privilèges de cette application correspondent aux profils permettant l'octroi d'accès et le traitement de la paie. Cependant, l'importance des accès d'un usager est multipliée si ce dernier possède également des droits de modification dans l'application Registre des postes (p. ex. modifier un salaire aux événements salariaux comme une promotion, une augmentation statutaire) ou dans l'application Time Sharing Option (interpréteur de lignes de commande utilisé sur les grands systèmes IBM (TSO)) sur l'ordinateur central qui permettent l'accès aux données directement. Les octrois d'accès à ces deux dernières applications ne sont pas sous la responsabilité de la direction de la paie.

[3] Un compte générique est un compte qui n'est pas attribué à un utilisateur en particulier. Il est généralement utilisé en cas d'urgence seulement par un groupe restreint d'administrateurs.

[4] Selon l'Office québécois de la langue française, la journalisation permet de garder la trace de certains événements en vue de vérifications ultérieures.

L'examen des comptes à hauts privilèges a révélé les faits saillants suivants :

- Trois usagers peuvent octroyer des accès dans l'application PAIE. Les autres usagers de cette application possèdent des profils permettant essentiellement de générer la paie, ce qui est normal compte tenu de leur travail;
- Deux usagers possèdent un accès à hauts privilèges dans les trois applications mentionnées ci-dessus (PAIE, Registre des postes et TSO). Ces personnes occupent le poste de coordonnateur paie. Ce ne sont toutefois pas tous les coordonnateurs paie qui ont la possibilité d'octroyer les accès dans l'application PAIE, ce qui est satisfaisant;
- De plus, nous avons relevé que 12 personnes possèdent des accès à hauts privilèges dans deux de ces applications (Registre des postes et TSO). Plusieurs de ces personnes sont des agents de contrôle administratifs de la paie et des avantages sociaux qui ont besoin de ces accès, notamment la possibilité de modifier un salaire aux événements salariaux.

Des contrôles administratifs de conciliation de la paie (p. ex. code à code) et des rapports d'exception sont révisés permettant de contrôler les usages de ces codes.

Nos travaux nous permettent de conclure que les accès privilégiés de cette application sont adéquatement octroyés et surveillés.

Aucune recommandation n'est nécessaire.

Application OASIS

Nous avons inventorié deux types de comptes à hauts privilèges donnant accès aux éléments suivants :

- La sécurité applicative;
- Les paramètres de l'application.

Notre audit nous a permis de constater que seules les personnes désignées comme intervenant au niveau de la sécurité possèdent les droits relatifs à celle-ci. En effet, une personne détient tous les droits dans l'application et deux autres personnes peuvent intervenir au niveau de la sécurité et l'octroi des accès, ce qui est acceptable. Toutes les actions posées en matière de sécurité font l'objet d'une journalisation et d'une révision quotidienne.

Nous avons également examiné les usagers ayant accès aux paramètres de l'application. Ils sont au nombre de neuf et ils travaillent comme programmeurs-analystes ou analystes-conseils au STI.

Nos travaux nous permettent de conclure que les accès privilégiés de cette application sont adéquatement octroyés et surveillés.

Aucune recommandation n'est nécessaire.

3.6. Tâches incompatibles

3.6.A. Contexte et constatations

Les bonnes pratiques en matière d'accès dictent qu'un usager ne doit pas être en mesure de contrôler l'ensemble d'un processus de l'organisation (p. ex. l'enregistrement des factures et leurs paiements).

En effet, la séparation des tâches incompatibles permet de détecter plus facilement les erreurs et prévient la fraude puisqu'elle rend plus difficile sa réalisation, car elle nécessite une collusion entre deux personnes ou plus.

Compte tenu de la nature de chacune des applications de notre audit, nous avons identifié des tâches incompatibles particulières et nous avons également analysé qui en détenait les droits d'accès.

Application SIMON

Pour cette application, nous avons tout d'abord examiné les responsabilités accordées dans chacun des arrondissements sur la base qu'une séparation de tâches est parfois plus difficile à réaliser compte tenu du nombre limité de personnes en poste.

Ensuite, nous avons examiné les accès à une combinaison de responsabilités qui, si elles sont détenues par le même usager, constituent des profils à risque.

Les combinaisons de responsabilités examinées sont :

- la saisie et le report d'écritures aux journaux de la Ville;
- la saisie des factures et la saisie des réceptions;
- la saisie des factures, le paiement et le déblocage des factures;
- la création de bons de commande et la saisie des réceptions.

Notre audit a révélé que des usagers détiennent des accès avec tâches incompatibles. Lorsque des accès sont attribués, malgré le fait qu'il existe un non-respect du principe de séparation de tâches, une dérogation doit être produite et approuvée. Les responsables des accès de l'application SIMON effectuent le suivi des dérogations avec une date de fin (des accès temporaires).

Pour les dérogations que nous avons observées, notre audit nous a révélé que ce sont des accès attribués pour des situations de relève, car les équipes sont restreintes ou pour des situations d'urgence. Dans ces cas, des contrôles compensatoires a posteriori sont effectués (p. ex. la production de rapports sur les transactions effectuées à l'aide de ces accès).

Par contre, nous avons constaté qu'il y a exception pour les 149 utilisateurs qui cumulent les deux responsabilités incompatibles, soit la création du bon de commande (SIMON – Atelier Acheteur PO) et la saisie des réceptions (SIMON – Achat en ligne ICX). En effet, ces tâches incompatibles permettent aux utilisateurs de créer à la fois des bons de commande et d'effectuer la réception de marchandises et de services. Bien que les demandes de dérogation aient été demandées et justifiées par leur gestionnaire, ces derniers ne font pas systématiquement un suivi des transactions effectuées par les détenteurs des deux profils. Or, un encadrement administratif sur la séparation des tâches stipule que les gestionnaires doivent effectuer un tel suivi.

Nous avons également été informés que dans le cadre d'un nouveau modèle d'affaires, le Service de l'approvisionnement prévoit centraliser l'émission des bons de commande au sein de son unité. Cette action assurera, entre autres, le respect de l'encadrement sur la séparation des tâches.

L'absence de mécanismes de surveillance des utilisateurs qui détiennent ces tâches incompatibles augmente le risque de transactions non autorisées.

RECOMMANDATION

3.6.B. Nous recommandons au Service de l'approvisionnement, dans le cadre du nouveau modèle d'affaires en approvisionnement, d'implanter un contrôle a posteriori afin de surveiller les opérations des utilisateurs cumulant les responsabilités incompatibles suivantes :

- **SIMON – Atelier Acheteur PO;**
- **SIMON – Achat en ligne ICX.**

RÉPONSE DE L'UNITÉ D'AFFAIRES

3.6.B. Service de l'approvisionnement

Avant la finalisation de la mise en place du nouveau modèle d'affaires du Service de l'approvisionnement, les actions suivantes seront entreprises :

- *Diffuser aux unités d'affaires une communication afin de rappeler l'encadrement et l'obligation d'effectuer les contrôles a posteriori par le rapport de contrôle conçu à cet effet;*
- *Avant le 31 mars 2020, renvoyer la liste des dérogations aux services concernés quant à la réévaluation et à la précision de la durée de la dérogation;*
- *Réévaluation périodique (trimestrielle) des dérogations et extraction des transactions non conformes.* ***(Échéancier prévu : au cours de l'année en cours, avec suivi le 31 décembre 2020)***

Application PAIE

Cette application ne possède pas de profils comportant des tâches incompatibles, car les opérations sont segmentées de façon à ce que les actions conflictuelles soient exécutées par une autre section ou par une application de la direction des ressources humaines. Comme mentionné à la section 3.5 « Comptes à hauts privilèges », le cumul d'accès à travers diverses applications peut rendre incompatible l'ensemble de ces droits détenus par un usager.

Notre audit nous a toutefois permis d'identifier que seulement deux usagers détiennent une combinaison d'accès à hauts privilèges. Ces accès sont justifiés compte tenu des tâches de ces usagers.

Nous estimons que les droits conflictuels sont gérés de façon satisfaisante pour cette application.

Aucune recommandation n'est nécessaire.

Application OASIS

Il existe également pour cette application de taxation, une forte segmentation des opérations en diverses sections opérationnelles. En effet, les opérations sont fonctionnellement divisées entre l'imposition, la perception et les encaissements. Les profils d'accès types sont créés à partir d'un ensemble de groupes d'écrans et de droits dans ceux-ci permettant à l'usager d'accomplir ses tâches.

Chaque type d'opérations possède des écrans propres à ses besoins. Par exemple, les accès pour l'imposition confèrent des droits d'intervenir au niveau des certificats d'évaluation. Au même titre, les écrans liés à la comptabilisation des encaissements ne devraient pas faire partie des accès disponibles aux personnes travaillant à l'imposition.

Pour chacune des opérations d'imposition, de perception et d'encaissements, nous avons validé qu'aucun profil d'accès ne permette la possibilité d'intervenir relativement aux écrans particuliers des autres groupes. De plus, nous avons vérifié qu'aucun utilisateur ne possédait un cumul de profils qui aurait permis de détenir ces accès incompatibles.

Nous concluons que les droits conflictuels sont gérés de façon satisfaisante pour cette application.

Aucune recommandation n'est nécessaire.

4. CONCLUSION

Selon nos travaux d'audit, nous concluons que le Service des technologies de l'information (STI), le Service des ressources humaines et le Service des finances gèrent respectivement les accès logiques aux applications SIMON, PAIE et OASIS de façon adéquate.

Les mécanismes de contrôle en place permettent de limiter les impacts d'accès non autorisés ou non appropriés en plus de restreindre les risques de fraude ou de collusion.

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

Critère d'évaluation – Gouvernance

La Ville de Montréal (la Ville) dispose d'encadrements couvrant les principaux domaines de la gestion des accès logiques et édictés par le STI. Cependant, certains doivent être mis à jour, car quelques paramètres ont été modifiés depuis leur rédaction et ils ne sont plus représentatifs de la réalité. En effet, certains principes de la gestion des accès logiques (les principes de privilège minimal, de séparation de tâches et de traçabilité) sont appliqués, mais ne sont pas présents au sein des encadrements.

Critère d'évaluation – Octroi des accès

Les accès accordés aux applications SIMON, PAIE et OASIS sont appropriés compte tenu des tâches de l'utilisateur. Des profils préétablis en fonction du poste occupé ont été définis pour les applications PAIE et OASIS. Pour l'application SIMON, un script lancé quotidiennement permet de retirer les accès aux usagers qui ont changé de postes.

Critère d'évaluation – Authentification et gestion des mots de passe

Les paramètres de mots de passe fixés pour l'authentification et la gestion des mots de passe sont adéquats pour les applications SIMON, PAIE et OASIS. Cependant, il n'existe aucun mécanisme d'identification a posteriori de la robustesse des mots de passe utilisés.

Critère d'évaluation – Surveillance et revue des accès

La surveillance et la revue des accès effectuées pour les applications SIMON, PAIE et OASIS sont adéquates. Pour les applications PAIE et OASIS, il y a une validation périodique formelle auprès des gestionnaires. De plus, tout accès non utilisé durant six mois est premièrement suspendu et par la suite détruit au niveau de la plateforme principale IBM. Notons toutefois que la revue des accès consentis au personnel des Bureaux Accès Montréal (BAM) pourrait s'effectuer plus fréquemment dans le cas de l'application OASIS.

Pour l'application SIMON, même s'il n'y a pas de validation périodique formelle auprès des gestionnaires, des scripts lancés quotidiennement, hebdomadairement et mensuellement permettent de détecter les anomalies d'accès et d'apporter les correctifs appropriés. De plus, tout accès à une fonction non utilisée dans un délai de six mois est automatiquement désactivé.

Critère d'évaluation – Comptes à hauts privilèges

Les comptes à hauts privilèges des applications SIMON, PAIE et OASIS sont en nombre limité et sont surveillés étroitement sauf pour l'application SIMON où la surveillance est manuelle et par conséquent inadéquate.

Critère d'évaluation – Tâches incompatibles

Les droits conflictuels sont gérés de façon satisfaisante pour les applications PAIE et OASIS. En effet, l'utilisation de profils d'accès préétablis de même que l'organisation opérationnelle du travail font en sorte que les situations qui pourraient être conflictuelles ne se retrouvent pas dans la même application ou sous la responsabilité d'une même section de leurs services respectifs.

Les droits conflictuels sont gérés de façon satisfaisante pour l'application SIMON, sauf pour les utilisateurs qui cumulent les responsabilités de création de bons de commande et de réception de biens et services. Dans ce cas, bien que les demandes de dérogation aient été dûment approuvées, les gestionnaires des unités d'affaires ne font pas de façon systématique de suivi a posteriori afin de vérifier que les usagers qui ont le double accès ne font pas de transactions non autorisées.

5. ANNEXE

5.1. Objectif et critères d'évaluation

Objectif

S'assurer que les accès logiques aux applications financières SIMON, PAIE et OASIS sont correctement gérés et limitent les risques d'accès non autorisés ou non appropriés en plus de restreindre les risques de fraude ou de collusion.

Critères d'évaluation

Nous avons basé notre audit sur les critères d'évaluation suivants répartis en six volets :

1. **Gouvernance**
   La Ville documente, communique et assigne les responsabilités de ses politiques et procédures en matière de gestion d'accès aux applications.
2. **Octroi des accès**
   Les unités administratives accordent les accès aux applications et les maintiennent uniquement s'ils sont conformes aux besoins.
3. **Authentification et gestion des mots de passe**
   La Ville dispose de paramètres de mots de passe robustes.
4. **Surveillance et revue des accès**
   Les unités administratives effectuent une revue périodique des accès accordés, permettant de retirer à leur détenteur les accès qui ne sont plus requis ou justifiés.
5. **Comptes à hauts privilèges**
   Les unités administratives accordent des accès privilégiés en nombre limité et uniquement aux utilisateurs qui ont besoin de ces accès.
6. **Tâches incompatibles**
   Les unités administratives s'assurent qu'un usager ne détient pas de droits d'accès lui permettant de contrôler de manière importante un processus transactionnel.