4.5.

GESTION DE L'APPLICATION GEM

LE 26 MARS 2019

SOMMAIRE DE L'AUDIT

OBJECTIF

Déterminer si les mécanismes de contrôle, mis en place pour l'application GEM, permettent de s'assurer que celle-ci ne présente aucun risque majeur de confidentialité, d'intégrité et de disponibilité des données quant à son cycle de vie, son utilisation et sa maintenance.

RÉSULTATS

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.

L'application GEM dispose des mécanismes de contrôles appropriés suivants :

- Les rôles et les responsabilités ainsi que le propriétaire de l'application GEM sont connus de tous;
- La sensibilisation du personnel aux risques de cybersécurité est correctement effectuée dans les différents départements;
- Les processus de gestion des incidents et de gestion des changements sont adéquats;
- Les paramètres de sécurité permettent des mots de passe robustes.

Néanmoins, les mécanismes de contrôle mis en place nécessitent des améliorations au niveau de la gestion des accès logiques. Ce constat combiné à la désuétude technologique et au manque de ressources humaines pourrait entraîner des risques de perte de confidentialité, de corruption de données et d'indisponibilité de l'application de gestion d'évaluation municipale (GEM).

Voici les éléments nécessitant des améliorations :

- Les rôles et les responsabilités ainsi que le propriétaire de l'application ne sont pas formalisés mais connus;
- Les formulaires de demandes d'accès ne sont pas conservés et les profils d'accès ne font pas l'objet de révision régulière;
- Le catalogue de changements mineurs non déployés est très important;
- L'équipe en charge de la modification de l'application est également responsable de déployer les changements en production;
- Les technologies utilisées à ce jour, ne sont plus maintenues par les vendeurs ou trop anciennes ce qui rend difficile le recrutement du personnel maîtrisant celles-ci;
- Dans le contexte d'une équipe réduite, l'attrition du personnel nécessite une attention particulière en raison des nombreux départs à la retraite prévus dans les 24 prochains mois;
- Il n'y a pas de processus formel de mise à jour de la documentation;
- Compte tenu de la vétusté de l'application GEM, des améliorations pourraient être apportées aux mécanismes de surveillance des accès;
- Un processus formel doit être mis en place pour une gestion plus efficace des problèmes;
- La surveillance applicative et celle de l'infrastructure doivent être renforcées pour une meilleure détection des pannes.

TABLE DES MATIÈRES

LISTE DES SIGLES

ASU
Agent Support Utilisateurs du service de l'évaluation foncière

CA
Application de gestion des incidents

FTP
Protocole de transfert de fichier *(File Transfer Protocol)*

GDM
Application de gestion des incidents et changements

GEM
Gestion de l'évaluation municipale

JIRA
Application de gestion des incidents et des changements technologiques de la ville

LFM
La loi sur la fiscalité municipale

Logiciel PG
Logiciel d'évaluation municipale utilisé par plusieurs villes du Québec

MAPAQ
Ministère de l'Agriculture, des Pêcheries et de l'Alimentation du Québec

RACI
Représente une matrice des responsabilités

SEF
Service d'évaluation foncière

STI
Service des technologies de l'information

TI
Technologies d'informations

1. CONTEXTE

Relevant de la Direction générale adjointe aux services institutionnels, le Service de l'évaluation foncière (SEF) a pour mission de confectionner, de tenir à jour et de défendre le rôle d'évaluation foncière des municipalités de l'agglomération de Montréal, conformément aux dispositions de la *Loi sur la fiscalité municipale* (LFM).

L'application Gestion de l'évaluation municipale (GEM) permet d'établir et de mettre à jour des rôles d'évaluation de la Ville de Montréal (la Ville). Ce rôle représente un inventaire de tous les immeubles sur le territoire d'une municipalité. Le parc immobilier de la Ville de Montréal représentait, en 2017, 438 000 unités évaluées à 274 milliards $. Un nouveau rôle d'évaluation est déposé tous les trois ans conformément à la *Loi sur la fiscalité municipale* et ses règlements afférents. L'application GEM permet également de procéder à l'émission des certificats de modification des unités d'évaluation. Des modules permettent de distribuer les tâches à effectuer par les employés et de contrôler les transactions venant modifier le rôle d'évaluation. Les données d'évaluation foncière de l'application GEM sont à la base des calculs de la taxation qui a généré un revenu de 4,2 milliards $ en 2017, représentant 76 % des revenus totaux non consolidés de la Ville.

Les principales obligations auxquelles sont soumises les activités du SEF et l'application GEM sont La LFM et ses règlements;

L'application GEM a été tout d'abord développée en 2004 par la Ville. Suite à quoi, la Ville de Québec s'est jointe à elle, en 2008. Elle a été modifiée régulièrement pour intégrer de nouvelles tâches telles que la gestion des permis. Depuis environ 2010, la Ville poursuit seule l'évolution de l'application GEM.

L'accès de l'interne à l'application GEM se fait au moyen d'un navigateur Internet. Des accès à distance sécurisés sont disponibles seulement pour quelques gestionnaires du SEF et pour les inspecteurs de la Ville. Aucun accès n'est possible à partir d'un réseau externe à la Ville. L'application GEM a une base de données sur Oracle en version 10G qui est hébergée sur un serveur de type Unix. L'outil Oracle Designer est utilisé pour le développement et permet de générer des écrans et des rapports. Il y a quatre environnements maintenus :

- Développement;
- Tests;
- Acceptation;
- Production.

Les principales interfaces entrantes à l'application GEM sont :

- Le Bureau de la publicité et des droits : les données sur les actes de vente, les jugements étant chargés par un fichier envoyé par courriel. Certaines informations sont enregistrées manuellement par le SEF;

- Les arrondissements : la plupart des arrondissements utilisent l'application de la Ville sur la gestion des permis;
- Les villes liées : la plupart des villes liées utilisent le logiciel PG (logiciel d'évaluation municipale utilisé par plusieurs villes du Québec). Certaines envoient encore leurs informations sur papier pour la transmission des permis;
- Le Service des incendies : les données concernant les unités d'évaluation qui ont subi un sinistre sont envoyées à l'application GEM (par une vue d'Oracle depuis le logiciel du Service des incendies);
- Le Service des finances : les mémos locatifs concernant les exemptions (p. ex. un immeuble appartenant au gouvernement fédéral) et les données des locataires de ces immeubles sont communiqués à l'application GEM.

Les principales interfaces sortantes à l'application GEM sont :

- Le Service des finances vers l'application OASIS : OASIS permet de gérer les comptes de taxes émis par la Ville à partir des données d'évaluation foncière. Un transfert hebdomadaire a lieu par le protocole *File Transfer Protocol* (FTP). L'application GEM est stratégique pour OASIS puisqu'il représente l'apport des données fondamentales aux calculs des taxes foncières;
- Villes liées : le données d'évaluation foncière les concernant sont envoyées par FTP;
- Le ministère des Affaires municipales et de l'Habitation (MAMH) : tous les rôles et certains certificats d'évaluation y sont envoyés.
- Le Conseil scolaire : les rôles et les certificats fonciers sont envoyés par FTP et servent à la taxation scolaire;
- Le ministère de l'Agriculture, des Pêcheries et de l'Alimentation du Québec (MAPAQ) : envoi des certificats concernant les exploitations agricoles enregistrées.

Les 170 utilisateurs actifs de l'application GEM sont soutenus par un pilote et trois agents support aux utilisateurs (ASU) du côté du SEF. Au Service des technologies de l'information (STI), il y a une analyste d'affaires, trois programmeurs et deux analystes TI qui sont responsables de l'application GEM.

Depuis l'automne 2018, un appel d'offres est en cours de rédaction (projet numéro 74551 au PTI de 2018) afin de moderniser et d'intégrer les applications GEM et OASIS, dans une même application. L'appel d'offres est actuellement en révision pour une publication au printemps 2019.

2. OBJECTIF DE L'AUDIT ET PORTÉE DES TRAVAUX

En vertu des dispositions de la *Loi sur les cités et villes*, nous avons réalisé une mission d'audit portant sur la gestion de l'application GEM, conformément à la norme canadienne de mission de certification NCMC 3001, du *Manuel de CPA Canada – Certification*.

Le présent audit avait pour objectif d'évaluer la gestion mise en place pour la gouvernance et la maintenance de l'application GEM afin de limiter les risques de perte d'informations, de corruption de données, de perte d'efficacité dans l'exploitation et dans l'évolution de l'application.

La responsabilité du vérificateur général de la Ville de Montréal consiste à fournir une conclusion sur les objectifs 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 en annexe.

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 sur les cinq critères d'évaluations suivants :

- Critère 1 — Rôles et responsabilités;
- Critère 2 — Gestion des accès logiques;
- Critère 3 — Gestion des changements;
- Critère 4 — Pérennité humaine et technique;
- Critère 5 — Gestion des opérations.

Nous avons exclu de notre mission les aspects afférents à la relève des TI et au processus de copies de sauvegarde, car ils ont été couverts lors de notre audit de 2015 sur la Gestion de la relève des technologies de l'information et des télécommunications. Des recommandations avaient été émises avec un échéancier de mise en place jusqu'au début 2020.

Notre audit a été réalisé du 16 juillet 2018 au 26 mars 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.

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 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. RÔLES ET RESPONSABILITÉS

3.1.A. CONTEXTE ET CONSTATATIONS

Afin de définir une imputabilité claire en matière des rôles et des responsabilités, ces derniers doivent être correctement définis, écrits et validés par toutes les parties concernées. Il est commun que ce processus donne naissance à une matrice RACI (Réalisateur, Approbateur, Consulté et Informé), servant de référence pour chaque processus de l'application tout au long de son cycle de vie. Elle peut servir de base si l'application est appelée à évoluer ou migrer vers un nouveau système.

De plus, pour chaque application, il est important de pouvoir définir qui sera la personne responsable de celle-ci, permettant une imputabilité claire pour chaque action nécessitant une chaîne de validation. Le responsable applicatif est le gardien du maintien en condition opérationnelle de l'application. Il doit être impliqué pour chaque changement majeur et pour chaque migration applicative.

Nous avons constaté qu'il n'existe pas de matrice (p. ex. la matrice RACI) définissant les rôles et les responsabilités. De plus, le propriétaire de l'application GEM n'est pas formellement identifié. Précisons, cependant, que les rôles et les responsabilités sont bien connus et respectés par chaque partie.

L'absence d'une matrice des rôles et des responsabilités pourrait engendrer des dysfonctionnements dans la gouvernance applicative tels que :

- la collaboration compliquée ou inefficace entre les équipes (p. ex les utilisateurs redirigés vers les mauvaises équipes pour la gestion des accès ou d'un incident);
- l'augmentation des erreurs humaines en production ou un délai dans les actions incombant aux équipes opérationnelles (p. ex. les actions exécutées deux fois en production, les suppressions);
- l'octroi de privilège applicatif sans cycle de validation.

RECOMMANDATION

3.1.B. Nous recommandons au Service des technologies de l'information conjointement avec le Service de l'évaluation foncière de créer une matrice des rôles et des responsabilités (p. ex. une matrice RACI) pour l'application de gestion de l'évaluation municipale. La matrice doit officialiser également le propriétaire de l'application.

RÉPONSE DES UNITÉS D'AFFAIRES

3.1.B. ***Service des technologies de l'information conjointement avec le Service de l'évaluation foncière***

Les rôles et les responsabilités sont connus tant du Service de l'évaluation foncière que du Service des technologies de l'information ainsi que le propriétaire de l'application.

Le livrable a consisté à produire une matrice RACI (représente une matrice des responsabilités) que nous avons transmise au Service de l'évaluation foncière pour commentaires. À l'intérieur du document nous avons officialisé le propriétaire de l'application. ***(Échéancier prévu : juin 2019)***

3.2. GESTION DES ACCÈS LOGIQUES

3.2.1. POLITIQUE DE GESTION DES ACCÈS

3.2.1.A. CONTEXTE ET CONSTATATIONS

Afin de prévenir des brèches de sécurité, des contournements d'accès et des abus de privilèges, un certain nombre de mesures, de documentations et de restrictions sont nécessaires.

De nombreux contrôles, processus et règlements doivent être établis pour prévenir les accès non autorisés ainsi que les usurpations d'identités.

Nous avons pris connaissance du processus mis en place pour la gestion des accès ainsi que les différents documents permettant de vérifier que l'attribution des droits privilégiés est correctement effectuée et surveillée.

Néanmoins, nous avons constaté les éléments suivants :

- Il n'existe pas de procédure de gestion des accès;
- Le processus d'octrois et de retraits des accès logiques est incomplet. En effet, les formulaires de demande et de validation ne sont pas archivés, empêchant une traçabilité des approbations;
- Le processus de révision des droits d'accès doit être formalisé;
- Il existe plusieurs comptes génériques qui ont des accès très restreints en production (limité à quelques écrans et en lecture uniquement). Ceux-ci ont une justification satisfaisante à l'exception d'un compte dont le contrôle est devenu difficile.

Bien que nous n'ayons pas trouvé des accès illégitimes lors de nos tests, sans gestion des accès formalisée et documentée, des droits d'accès inappropriés pourraient être octroyés ou conservés et pourraient mener à des erreurs ou à des fraudes. L'utilisation de comptes génériques mal contrôlés rendrait difficile l'imputabilité des utilisateurs de ces comptes en cas d'actions inappropriées.

RECOMMANDATION

3.2.1.B. **Nous recommandons au Service de l'évaluation foncière de :**

- **créer une procédure pour la gestion des accès;**
- **conserver les formulaires dûment approuvés de demande et de retraits des accès;**
- **formaliser le processus de révision des accès et de leurs droits;**
- **revoir la gestion des comptes génériques et la redéfinition de ces derniers. Chaque création de comptes générique doit être associée à un formulaire de dérogation correctement documenté et approuvé.**

RÉPONSE DE L'UNITÉ D'AFFAIRES

3.2.1.B. ***Service de l'évaluation foncière***

La procédure déjà en place sera revue et améliorée, détaillée formellement dans un document et diffusée aux personnes visées. ***(Échéancier prévu : 30 mai 2019)***

Les formulaires seront revus et un mode de conservation des demandes sera mis en place. ***(Échéancier prévu : 30 mai 2019)***

Une révision informelle des accès est réalisée périodiquement mais plutôt informellement. Elle sera systématisée et la fréquence de révision sera établit. ***(Échéancier prévu : 30 mai 2019)***

La gestion des comptes génériques est déjà en cours de révision, tous les droits d'accès auront été revus et formalisés d'ici le 15 mai 2019.

3.2.2. ROBUSTESSE DES MOTS DE PASSE

3.2.2.A. CONTEXTE ET CONSTATATIONS

Afin de disposer de mots de passe robustes, il est important d'établir des règles de sécurité sur leur usage. En effet, lors d'une cyberattaque, il est facile de compromettre des mots de passe s'ils sont d'une complexité très faible.

Nous avons constaté que les règles de sécurité des mots de passe de l'application GEM sont adéquates, puisqu'elles suivent les saines pratiques de l'industrie.

Cependant, compte tenu de la vétusté de l'application GEM, des améliorations pourraient être apportées aux mécanismes de surveillance des accès.

3.2.3. SÉGRÉGATION DES DROITS D'ACCÈS

3.2.3.A. CONTEXTE ET CONSTATATIONS

Afin de prévenir des accès non autorisés ou des fraudes dans l'application GEM, il est important de maintenir une ségrégation des droits entre les profils et les droits accordés. Dans ce contexte, les attributions de comptes à hauts privilèges doivent être parfaitement réglementées et suivies.

Nous avons constaté que la définition des différents profils de l'application GEM permet une bonne ségrégation des droits et un contrôle adéquat des accès. Ainsi, les profils sont définis en fonction des postes occupés par les utilisateurs. Cependant, ils ne font pas l'objet d'une révision régulière.

Sans une révision régulière des profils et des droits d'accès afférents, cela pourrait mener à ce que des utilisateurs disposent de droits d'accès permettant de contrôler des étapes clés d'une transaction ou d'un évènement (p. ex. de modifier une évaluation et d'autoriser la modification).

RECOMMANDATION

3.2.3.B. Nous recommandons au Service de l'évaluation foncière de mettre en place un processus récurrent de révision des profils d'accès et de leurs droits.

RÉPONSE DE L'UNITÉ D'AFFAIRES

3.2.3.B. ***Service de l'évaluation foncière***

Un processus de révision des droits que confèrent chacun des profils d'utilisateurs existants sera défini. La révision sera effectuée annuellement, ou à chaque fois qu'un processus ou que les rôles et les responsabilités d'un corps d'emploi sera modifié. ***(Échéancier prévu : 30 mai 2019)***

3.2.4. SENSIBILISATION À LA CYBERSÉCURITÉ

3.2.4.A. CONTEXTE ET CONSTATATIONS

Pour un contrôle et des mesures de sécurité appropriées, la sensibilisation du personnel et une formation sur les sujets en matière de cybersécurité doivent se faire de manière périodique afin de prévenir des compromissions et des vulnérabilités de sécurité en interne.

Nous avons constaté que la Ville dispose d'un département dédié à la cybersécurité et à mis en place un portail de sensibilisation et de formation à la disposition des employés.

Nous avons consulté le contenu, les fréquences de mise à jour du portail, ainsi que la planification régulière de formations et des ateliers de sensibilisation. L'examen de ces éléments nous permet de conclure que le personnel est correctement sensibilisé et formé pour gérer des situations de cybersécurité.

Aucune recommandation n'est nécessaire.

3.3. GESTION DES CHANGEMENTS

3.3.1. PROCESSUS DE GESTION DES CHANGEMENTS

3.3.1.A. CONTEXTE ET CONSTATATIONS

Toute modification dans un environnement de production doit suivre un certain nombre de réglementations, de processus et de validations. En effet, sans processus et de contrôles adaptés, l'intégrité et la stabilité de l'application seraient à risque. L'utilisation d'outils appropriés pour le suivi, le contrôle et la surveillance est primordiale.

Nous avons constaté les éléments suivants :

- La gestion des changements est documentée de manière appropriée et les outils utilisés par les équipes du SEF et du STI sont adéquats;
- Les changements sont correctement documentés et approuvés par les outils de gestion des changements (JIRA et GDM);
- Les phases de test et le cycle d'approbation sont respectés;
- Un suivi des priorités, de planification et de surveillance est effectué pour chaque changement mis en production.

Cependant, nous avons constaté que le catalogue de changements non déployé est considérable (plus de 400 changements) et pourrait être amené à augmenter davantage sans réaction appropriée pour y remédier.

Bien que ces changements non déployés soient mineurs, leur accumulation engendre des risques, car il autorise l'amoncellement de tâches de contournement qui pourraient mener à un problème plus important.

RECOMMANDATION

3.3.1.B. Nous recommandons au Service des technologies de l'information conjointement avec le Service de l'évaluation foncière d'analyser la liste des changements non déployés en production pour comprendre les problématiques et ainsi servir de base de connaissance pour la nouvelle application.

RÉPONSE DES UNITÉS D'AFFAIRES

3.3.1.B. ***Service des technologies de l'information conjointement avec le Service de l'évaluation foncière***

Nous avons mis plus de six mois pour la préparation de l'appel d'offres de remplacement de la Gestion de l'évaluation municipale, notamment les grilles de fonctionnalités et ce, en collaboration intense avec le Service de l'évaluation foncière.

Le devis de l'appel d'offres englobe plus de 180 cas d'utilisation spécifiques à l'évaluation foncière, incluant les demandes de changements non déployés en production. Ceci couvre l'ensemble des fonctionnalités souhaitées par le client dans la nouvelle application.

Le livrable consistera donc à ajouter à même la liste des changements non déployés, un statut (inclus dans l'appel d'offres) Il y a plus de 400 demandes de changements répertoriés. ***(Échéancier prévu : juin 2019)***

3.3.2. RESTRICTION DES DROITS EN PRODUCTION

3.3.2.A. CONTEXTE ET CONSTATATIONS

Il est commun de voir des erreurs de changements, dans un environnement de production au lieu d'un environnement de tests, par l'équipe de programmeurs, car ces derniers ont des droits d'écriture dans ces deux environnements. Il devient également possible pour un programmeur de contourner les processus officiels lorsqu'il dispose d'un accès direct en production.

En consultant la liste des utilisateurs en production avec leurs droits associés, nous constatons que l'équipe en charge de la modification du logiciel (le programmeur) et celle responsable de déployer les changements (l'exploitation) est la même. De ce fait, il est impossible de mettre en place une ségrégation des droits appropriée. Selon notre compréhension, la taille réduite des équipes constitue une limite pour appliquer ce principe.

Sans une restriction congrue des droits en production, les programmeurs pourraient déployer des changements non autorisés en production. L'intégrité de l'application pourrait en être compromise.

RECOMMANDATION

3.3.2.B. Nous recommandons au Service de l'évaluation foncière conjointement avec le Service des technologies de l'information de mettre en place un contrôle compensatoire (p. ex. un rapport des mises en production) afin de s'assurer que toutes les mises en productions ont bien été approuvées par le comité de validation des changements.

RÉPONSE DES UNITÉS D'AFFAIRES

3.3.2.B. ***Service de l'évaluation foncière conjointement avec le Service des technologies de l'information***

Tel que mentionné dans le rapport, la taille réduite de l'équipe constitue une limite dans le cloisonnement des rôles lors des mises en production.

Le livrable consistera d'ajouter un rapport des mises en production qui sera révisé et approuvé par le chef de division et par le client.
(Échéancier prévu : septembre 2019)

3.3.3. CONFORMITÉ AUX LOIS

3.3.3.A. CONTEXTE ET CONSTATATIONS

L'application GEM se doit de suivre et d'intégrer les modifications aux lois et réglementations afférentes à l'évaluation foncière. Sans cela la conformité législative de l'application peut être mise en péril.

Nous avons constaté que les changements liés aux différentes lois et réglementations avaient été correctement priorisés et implantés en temps opportun.

Aucune recommandation n'est nécessaire.

3.4. PÉRENNITÉ HUMAINE ET TECHNIQUE

3.4.A. CONTEXTE ET CONSTATATIONS

Pour assurer une utilisation adéquate et optimale pour les utilisateurs, une application doit faire l'objet d'inspections, de mises à niveau et de documentations à jour. L'accumulation d'une dette technologique peut rendre la maintenabilité de l'application GEM très complexe et en réduire la performance.

Nous avons constaté les éléments suivants :

- L'application n'a pas évolué technologiquement depuis sa création en 2004;
- Les versions de base de données utilisées sont désuètes et elles ne sont plus soutenues par le fournisseur, impliquant l'accumulation potentielle de vulnérabilités majeures;
- En raison de cette désuétude, le recrutement de nouvelles ressources est plus difficile étant donné les prérequis technologiques nécessaires;
- La taille des équipes d'exploitation est également déjà très réduite, à ce jour (5 personnes pour 170 utilisateurs). Compte tenu des départs à la retraite au cours des 24 prochains mois, il sera difficile de maintenir l'exploitation opérationnelle de l'application.

Une perte de connaissances et de maîtrise de l'application pourrait survenir, si la gestion de l'attrition du personnel n'est pas correctement effectuée. Sans gestion de la dette technologique de l'application GEM, il serait difficile de la maintenir opérationnelle jusqu'au projet de remplacement. Également, les mises à jour de sécurité n'étant plus émises par le fournisseur, l'application pourrait être à risque en cas de cyberattaque du fait de la présence de vulnérabilités non corrigées.

RECOMMANDATION

3.4.B. **Nous recommandons au Service des technologies de l'information conjointement avec le Service de l'évaluation foncière de :**

- **prioriser le projet du remplacement de l'application de gestion de l'évaluation foncière afin de ne plus subir la dette technologique accumulée lors de ces dernières années;**
- **définir un plan de relève assurant un nombre de ressources suffisantes et le transfert de connaissances afin de maintenir l'application de gestion d'évaluation municipale jusqu'à la réalisation de son projet de remplacement.**

RÉPONSE DES UNITÉS D'AFFAIRES

3.4.B. ***Service des technologies de l'information conjointement avec le Service de l'évaluation foncière***

Le projet de remplacement fait partie de notre feuille de route des projets priorisés et doit obtenir l'aval du comité du directeur général. Le plan sera présenté dans la semaine du 6 mai au directeur général adjoint responsable du Service des technologies de l'information et par la suite au directeur général et ce, afin d'obtenir les budgets nécessaires.

En ce qui concerne le plan de relève, une réévaluation des ressources requises pour l'exploitation est en cours, et des recommandations seront acheminées à la Direction générale adjointe des Services aux citoyens. ***(Échéancier prévu : septembre 2019)***

3.5. GESTION DES OPÉRATIONS

3.5.1. DOCUMENTATION APPLICATIVE

3.5.1.A. CONTEXTE ET CONSTATATIONS

Afin d'assurer une efficacité opérationnelle et une maintenabilité de l'application, il est important de disposer d'une documentation claire et à jour. Cette documentation doit être vérifiée et indexée régulièrement pour en assurer une traçabilité adéquate.

Nous avons constaté les éléments suivants :

- Il existe une documentation applicative pertinente des opérations (incluant le contrôle des procédures automatisées);
- Bien que cette documentation ait été actualisée en septembre 2018, il n'y a aucun processus de mise à jour.

Sans processus de mise à jour de la documentation, celle-ci pourrait devenir obsolète et une perte progressive de la connaissance pourrait se produire. Par conséquent, les risques de panne de l'application pourraient être augmentés de même que leurs délais de résolution.

RECOMMANDATION

3.5.1.B. **Nous recommandons au Service des technologies de l'information d'implanter un processus de mise à jour de la documentation applicative.**

RÉPONSE DE L'UNITÉ D'AFFAIRES

3.5.1.B. ***Service des technologies de l'information***
Le Service des technologies de l'information nous a confirmé qu'il est en accord avec la recommandation qui lui est adressée. Le plan d'action détaillé suivra sous peu.

3.5.2. GESTION DES INCIDENTS

3.5.2.A. CONTEXTE ET CONSTATATIONS

Dans le cycle de vie d'une application, chaque incident détecté en production doit être correctement documenté dans une application de billetterie facilitant l'identification unique de l'incident en documentant l'origine du problème, les impacts et sa résolution.

Nous avons constaté que les incidents enregistrés dans les outils GEM ou Jira sont documentés et suivis correctement selon le cycle de vie d'un incident (la création, les tests, la communication, la résolution et la clôture).

Aucune recommandation n'est nécessaire.

3.5.3. GESTION DES PROBLÈMES

3.5.3.A. CONTEXTE ET CONSTATATIONS

Un problème est la récurrence d'un incident nécessitant un plan d'action pour sa correction. Pour chaque problème, ce plan doit être suivi de manière périodique afin de s'assurer de la bonne mise en place des actions correctives et de la bonne progression de celui-ci.

Nous avons constaté que les problèmes sont bien notés dans le système de billetterie, mais, qu'à ce jour, il n'existe pas de processus de gestion des problèmes avec le suivi nécessaire associé.

L'absence de ce processus pourrait mener à des faiblesses dans la mise en place d'un plan d'action nécessitant un suivi rigoureux et les problèmes pourraient ne pas être corrigés en temps opportun.

RECOMMANDATION

3.5.3.B. **Nous recommandons au Service des technologies de l'information de mettre en place un processus de gestion des problèmes pour l'application de gestion de l'évaluation foncière.**

RÉPONSE DE L'UNITÉ D'AFFAIRES

3.5.3.B. ***Service des technologies de l'information***
Le Service des technologies de l'information nous a confirmé qu'il est en accord avec la recommandation qui lui est adressée. Le plan d'action détaillé suivra sous peu.

3.5.4. SURVEILLANCE APPLICATIVE ET DE L'INFRASTRUCTURE

3.5.4.A. CONTEXTE ET CONSTATATIONS

L'infrastructure et les processus sensibles de l'application GEM doivent faire l'objet d'une surveillance d'incidents et d'une continuité de services appropriés afin de réduire les délais de panne et de garantir une remontée de l'information rapide aux différentes parties prenantes de l'application. Pour cela, les écrans critiques de l'application ainsi que l'infrastructure (incluant les serveurs et les bases de données) doivent faire l'objet d'une surveillance par les équipes d'exploitation.

Nous avons constaté qu'il n'y avait pas d'outils ni de rapports permettant une détection efficace des ralentissements de service ou des pannes sur les écrans critiques applicatifs ou concernant l'infrastructure de l'application GEM.

Sans surveillance préventive des écrans critiques applicatifs et de l'infrastructure, les équipes d'exploitation n'auraient pas la réactivité nécessaire pour pallier à un incident majeur. Le délai de résolution serait allongé.

RECOMMANDATION

3.5.4.B. **Nous recommandons au Service des technologies de l'information de mettre en place un processus de surveillance de l'application de gestion de l'évaluation foncière qui devra inclure, entre autres, la surveillance des écrans critiques et la surveillance des serveurs et des bases de données.**

RÉPONSE DE L'UNITÉ D'AFFAIRES

3.5.4.B. ***Service des technologies de l'information***

Le Service des technologies de l'information nous a confirmé qu'il est en accord avec la recommandation qui lui est adressée. Le plan d'action détaillé suivra sous peu.

4. CONCLUSION

Il est important de mentionner que l'application de gestion d'évaluation municipale (GEM) fournit les données nécessaires à la production de la taxation qui a généré en 2017 un revenu de 4,2 milliards $, soit 76 % des revenus totaux non consolidés de la Ville.

L'application GEM dispose de mécanismes de contrôle approprié quant à la connaissance des rôles et des responsabilités par les intervenants, à la sensibilisation du personnel aux risques de cybersécurité, aux processus de gestion des incidents et des changements et aux paramètres de sécurité des mots de passe.

Néanmoins, les mécanismes de contrôle mis en place nécessitent des améliorations au niveau de la gestion des accès logiques. Ce constat combiné à la désuétude technologique et au manque de ressources humaines pourrait entraîner des risques de perte de confidentialité, de corruption de données et d'indisponibilité de l'application GEM.

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

Critère 1 : rôles et responsabilités

Les rôles et les responsabilités ainsi que le propriétaire de l'application sont connus de tous. Néanmoins, ceux-ci ne sont pas formalisés.

Critère 2 : gestion des accès logiques

Concernant la politique de gestion des accès, nous notons quelques axes d'améliorations. En effet, les formulaires de demande d'accès ne sont pas conservés. Il est à noter que la procédure de création des profils et le processus de revue des comptes utilisateurs doivent être formalisés. Enfin, la gestion des comptes génériques n'est pas correctement encadrée.

La robustesse des mots de passe permet la sécurisation de ces derniers. Cependant, compte tenu de la vétusté de l'application GEM, des améliorations pourraient être apportées aux mécanismes de surveillance des accès.

La ségrégation des droits d'accès fait preuve d'une définition adéquate permettant une bonne attribution des droits en fonction du profil utilisateur. En revanche, ces profils ne font pas l'objet de révision régulière.

La sensibilisation du personnel aux risques de cybersécurité est correctement effectuée dans les différents départements. Le portail et les différentes campagnes de sensibilisation à disposition sont des outils efficaces pour se prémunir de ce type de risque.

Critère 3 : gestion des changements

Ce processus respecte chaque étape du cycle de vie d'une demande de changement (de la demande, en passant par les tests pour terminer par la mise en production). L'implantation des changements liés à une nouvelle réglementation ou loi est effectuée en temps opportun.

Cependant, nous avons remarqué que le catalogue des changements mineurs non déployés et en attente est très important.

Également, l'équipe en charge de la modification de l'application est également responsable de déployer les changements en production.

Critère 4 : pérennité humaine et technique

L'application GEM accumule une dette technologique très importante nécessitant un plan d'action pour pallier à la désuétude. Les technologies utilisées à ce jour ne sont plus maintenues par les vendeurs ou trop anciennes pour avoir du personnel maîtrisant celles-ci. De plus, l'attrition du personnel nécessite une attention particulière étant donné les nombreux départs à la retraite prévus au cours des 24 prochains mois.

Critère 5 : gestion des opérations

Concernant la gestion des opérations, la documentation applicative existe, mais elle ne fait pas l'objet d'un processus de mise à jour.

La gestion des incidents est appropriée. Un processus formel doit être mis en place pour une gestion plus efficace des problèmes. Enfin la surveillance applicative et de l'infrastructure doivent être renforcées pour une meilleure détection des pannes et ainsi augmenter la réactivité des équipes.

5. ANNEXE

5.1. OBJECTIF ET CRITÈRES D'ÉVALUATION

OBJECTIF

Déterminer si les mécanismes de contrôle mis en place pour l'application GEM permettent de s'assurer que celle-ci ne présente aucun risque majeur de confidentialité, d'intégrité et de disponibilité des données quant à son cycle de vie, son utilisation et sa maintenance.

CRITÈRES D'ÉVALUATION

Critère 1 : rôles et responsabilités

Les rôles et les responsabilités sont définis, approuvés et communiqués permettent une imputabilité claire (p. ex. la matrice RACI). Un propriétaire de l'application GEM est formellement identifié.

Critère 2 : gestion des accès logiques

La gestion des accès doit être correctement documentée et doit inclure une revue périodique des accès. L'application GEM utilise des paramètres d'authentification assez robustes pour maintenir un environnement sûr. Le risque d'accès non autorisé peut augmenter, dans le cas contraire. Les profils et les droits accordés permettent une ségrégation adéquate afin de prévenir des accès non autorisés ou des fraudes. Des activités de surveillance doivent être mises en place afin de détecter des incidents en temps opportun.

Critère 3 : gestion des changements

Tout changement en production doit être proprement documenté, tracé, testé et validé par les autorités compétentes. L'accès des programmeurs à l'environnement de production est restreint. Les modifications de l'environnement de production sont surveillées. Les modifications aux lois et aux règlements sont intégrées en temps opportun à l'application GEM.

Critère 4 : pérennité humaine et technique

Tout au long de son cycle de vie applicative, il est important de limiter la dette technologique, d'assurer une documentation adéquate, de disposer de suffisamment de personnel qualifié pour maintenir une exploitation de l'application sans risque majeur (p. ex. des arrêts des systèmes intempestifs et répétés).

Critère 5 : gestion des opérations

L'application GEM dispose d'une documentation permettant de minimiser les risques opérationnels. Chaque incident en production fait part d'un ticket unique qui retrace l'origine, le problème et sa résolution. Un plan d'action est associé aux problèmes et aux incidents de type majeur. L'infrastructure et les processus importants de l'application GEM sont correctement surveillés.