



Bureau du vérificateur général

Rapport sur les suivis de vérification

Déposé devant le Comité de la vérification

Le 29 mai 2019



Bureau du vérificateur général

Le 29 mai 2019

Au maire, aux membres du Comité de la vérification et aux membres du Conseil,

C'est avec plaisir que je vous présente le rapport sur les suivis de vérification effectués par le Bureau du vérificateur général de la Ville d'Ottawa.

Le rapport inclut un aperçu et un sommaire de chacun des suivis effectués.

Le tout respectueusement soumis,

A handwritten signature in black ink that reads 'Ken Hughes'.

Ken Hughes

Vérificateur général



Personnel du Bureau du vérificateur général

Ken Hughes

Sonia Brennan

Ed Miner

Chantal Amyot

Abhishek Gangwal

Sarah Parr

Louise Proulx

Margaret Sue

Nathan Sassi

Ines Santoro

Table des matières

Progrès réalisés.....	1
Sommaire et évaluation de l'état de mise en œuvre global des recommandations du rapport de vérification	1
Sommaires – Suivis de vérification	5
Suivi de la vérification de 2015 de l'Unité des comptes créditeurs	6
Suivi de la vérification de 2015 du Projet de lecture automatisée des compteurs d'eau	11
Suivi de la vérification de 2014 des opérations hivernales : planification de la capacité et indicateurs de rendement	13
Suivi de la vérification de 2015 de la gouvernance des technologies de l'information	16
Suivi de la vérification de 2015 de la gestion des risques liés aux technologies de l'information	24

Progrès réalisés

Le Bureau du vérificateur général (BVG) assure le suivi de ses vérifications deux ou trois ans après le dépôt de son rapport afin de donner à la direction le temps de mettre en œuvre ses recommandations. Un suivi peut être mené plus tôt si la mise en œuvre des mesures correctives est achevée. Le BVG respecte les pratiques exemplaires et les normes professionnelles de la communauté internationale des vérificateurs en incluant la pratique du suivi de vérification. Le processus de vérification comprend différentes étapes : la planification, le travail sur le terrain, la production du rapport et, enfin, le suivi. À l'étape du suivi, le BVG évalue l'adéquation, l'efficacité et le caractère opportun des mesures que la direction a prises pour donner suite aux observations et aux recommandations inscrites dans le rapport de vérification. Cette évaluation permet au Bureau de s'assurer que les mesures requises, promises par la direction et approuvées par le Conseil ont été mises en œuvre. En conséquence, les suivis décrits dans le présent rapport ont été effectués selon les plans de travail 2017 et 2018 du Bureau du vérificateur général.

Les suivis des vérifications figurant dans le présent rapport comprennent les suivants :

- Vérification de l'Unité des comptes créditeurs
- Vérification du Projet de lecture automatisée des compteurs d'eau
- Vérification des opérations hivernales : planification de la capacité et indicateurs de rendement
- Vérification de la gouvernance des technologies de l'information
- Vérification de la gestion des risques liés aux technologies de l'information
- Vérification de la gestion des incidents de sécurité des TI et des interventions connexes (présentée à huis clos)

Comme on peut le voir dans la section suivante, il est clair, d'après les résultats de ces suivis, que la direction participe activement au processus de vérification.

Sommaire et évaluation de l'état de mise en œuvre global des recommandations du rapport de vérification

Les vérifications aident à améliorer les pratiques de gestion, à augmenter l'efficacité opérationnelle, à cibler les économies potentielles et à régler un certain nombre de problèmes précis. L'étape du suivi permet d'évaluer le degré de mise en œuvre des recommandations formulées dans les rapports de vérification. Le présent rapport ne

visé pas à fournir une évaluation de chacune des recommandations formulées. Il présente plutôt notre évaluation globale des progrès réalisés à ce jour à la suite de toutes les vérifications effectuées. Le personnel du BVG se tient à la disposition du Conseil si ce dernier souhaite tenir une discussion plus approfondie sur certains suivis.

Le tableau ci-dessous résume notre évaluation de l'état de mise en œuvre de chaque recommandation pour les suivis de vérification susmentionnés.

Tableau 1 : Sommaire de l'état de mise en œuvre des recommandations

Suivi	Total	Achevée	En cours	À venir	Impossible à évaluer	Ne s'applique plus
Unité des comptes créditeurs	7	2	3	1	0	1
Projet de lecture automatisée des compteurs d'eau	4	4	0	0	0	0
Opérations hivernales : planification de la capacité et indicateurs de rendement	20	17	3	0	0	0
Gouvernance des technologies de l'information	9	4	5	0	0	0
Gestion des risques liés aux technologies de l'information	8	0	7	0	1	0

Suivi	Total	Achevée	En cours	À venir	Impossible à évaluer	Ne s'applique plus
Gestion des incidents de sécurité des TI et des interventions connexes	11	6	4	0	1	0
Total	59	33	22	1	2	1
Pourcentage	100 %	56 %	37 %	2 %	3 %	2 %

Nous avons classé chacun des suivis de vérification d'après les critères suivants :

- **Solides progrès** = 50 % ou plus des recommandations évaluées comme étant « achevées »;
- **Peu ou pas de progrès** = 50 % ou plus des recommandations évaluées comme étant « à venir »;
- **Progrès graduels** = tous les autres suivis.

Solides progrès

- Vérification du Projet de lecture automatisée des compteurs d'eau
- Vérification des opérations hivernales : planification de la capacité et indicateurs de rendement
- Vérification de la gestion des incidents de sécurité des TI et des interventions connexes

Peu ou pas de progrès

- Aucun

Progrès graduels

- Vérification de l'Unité des comptes créditeurs
- Vérification de la gouvernance des technologies de l'information
- Vérification de la gestion des risques liés aux technologies de l'information

En raison de l'importance des questions en suspens relatives aux suivis de vérification liés aux technologies de l'information, le Bureau du vérificateur générale effectuera un examen supplémentaire pour assurer la mise en œuvre intégrale des recommandations. Selon le plan de travail annuel et les demandes du Conseil municipal, de nouvelles vérifications dans ces domaines pourraient avoir lieu à l'avenir.

Sommaires – Suivis de vérification

La section suivante contient le sommaire de chacun des suivis de vérification.

Suivi de la vérification de 2015 de l'Unité des comptes créditeurs

Le suivi de la vérification de 2015 de l'Unité des comptes créditeurs faisait partie du plan de travail 2017 du Bureau du vérificateur général.

Cette vérification avait à l'origine permis de cerner des occasions, pour la Ville, de solidifier les contrôles de l'Unité des comptes créditeurs (UCC) et de faire appel à la technologie pour accroître l'efficacité dans le traitement des factures, pour maximiser les économies de coûts et pour surveiller le rendement. Voici les principales constatations découlant de la vérification menée à l'origine :

- Les rôles, les responsabilités et la redevabilité des parties prenantes de l'UCC sont bien définis et compris et sont étayés par des normes, des procédures et des outils.
- L'UCC applique un processus de gestion des risques qui cadre avec la Politique sur la gestion améliorée des risques (GAR) de la Ville et qui permet de repérer, d'évaluer, d'atténuer et de surveiller continuellement les risques.
- La division des tâches¹ (DT) est nécessaire pour maîtriser le risque d'erreurs ou de fraudes potentielles. Dans les cas où le personnel de l'UCC doit avoir des droits d'accès qui débordent ceux qui ont été attribués à leur poste, il faut procéder à un examen des problèmes potentiels de la DT avant d'attribuer des droits d'accès supérieurs. Bien que ce processus ait été expliqué de vive voix, il n'a pas été possible de démontrer qu'il a été appliqué uniformément et rigoureusement.
- Dans le système SAP, un champ peut être configuré pour lancer une vérification des factures en double pour tous les fournisseurs, avant de régler les factures. Ce contrôle de l'application est configuré comme une fonction optionnelle et n'est pas automatiquement exercé obligatoirement pour tous les fournisseurs. Les employés de l'UCC doivent donc sélectionner ce champ manuellement lorsqu'ils créent ou mettent à jour un fichier de fournisseur. Sinon, il y a un risque que des

¹ La division des tâches (DT) est obligatoire pour la gestion permanente des risques et les contrôles internes de l'organisme. Le principe de la DT se fonde sur la responsabilité partagée d'un processus essentiel qui a pour effet de répartir les fonctions critiques de ce processus parmi plusieurs personnes ou directions générales. (Source : aicpa.org)

paiements en double soient traités pour des fournisseurs, et il faut alors s'en remettre à des contrôles compensatoires manuels pour les repérer.

- Le système SAP comprend des renseignements essentiels sur les fournisseurs de la Ville dans les champs du « fichier principal des fournisseurs ». La mise à jour de ces champs est essentielle, puisque les renseignements confidentiels comme les coordonnées bancaires y sont conservés et permettent de traiter les paiements. Pour avoir accès à ces renseignements et pour pouvoir les modifier, il faut prévoir des contrôles rigoureux afin de maîtriser le risque de fraude potentielle. Quand un employé crée un nouveau fournisseur ou met à jour les renseignements sur un fournisseur existant dans SAP, les modifications entrent en vigueur. On n'a pas défini de champ de données confidentielles à faire obligatoirement approuver avant que les modifications entrent en vigueur dans le système.
- Les retards dans l'examen et l'approbation des factures entraînent d'autres retards dans le traitement des paiements et privent la Ville de rabais². L'UCC a mis en œuvre une fonctionnalité prioritaire dans MarkView³ pour signaler aux utilisateurs les dates d'échéance des rabais potentiels. Nous avons constaté que malgré cette fonctionnalité, les avis ne permettent pas de distinguer les factures absolument prioritaires dans les cas où le rabais offert arrive à échéance ou que l'échéance d'une facture est proche. Pour mettre en évidence ces factures et permettre à l'utilisateur opérationnel d'y attribuer des priorités pour intervenir immédiatement, il faudrait éclaircir le message de ces avis.
- Bien que l'on surveille le montant de rabais dont la Ville a été privée, on ne fait pas de repérage des pénalités à la suite de retards de paiement.
- Bien que l'on surveille le rendement de l'UCC pour l'ensemble de l'administration municipale, on donne, aux unités opérationnelles, de l'information analytique et comptable limitée sur leurs résultats. La Ville a l'occasion de miser sur les outils

² Les factures de certains fournisseurs prévoient un rabais si le paiement est effectué dans un certain délai ou avant une date définie.

³ MarkView est le système dont se sert la Ville d'Ottawa pour automatiser le traitement des factures. Dans le cadre de ce processus, la Ville reçoit les factures des fournisseurs et prend connaissance des champs clés de ces factures pour les traiter. Lorsque les factures sont traitées, le commis de l'UCC passe en revue les détails des transactions dans MarkView par rapport aux factures d'origine pour s'assurer que les renseignements sont complets et exacts avant le processus de vérification et de paiement.

et les analyses de l'UCC pour adresser périodiquement aux unités opérationnelles des rapports sur leurs résultats relativement aux rabais dont la Ville peut se prévaloir, mais dont elle ne profite pas, aux paiements en retard, et aux délais moyens d'approbation des factures.

- On peut faire appel à l'automatisation pour accroître l'efficacité et l'efficacité de l'approbation et du traitement des factures des fournisseurs. On a l'occasion de mieux utiliser la technologie pour assurer la surveillance automatisée des rabais en fonction des dates de réception ou d'acceptation des factures. On peut configurer la technologie de la numérisation pour capter plus fidèlement les renseignements dans les factures et réduire l'importance des interventions manuelles à effectuer.

Tableau 1 : Sommaire de l'état de la mise en œuvre des recommandations

Recommandations	Total	Achevées	En cours	À venir	Ne s'appliquent plus
Nombre	7	2	3	1	1
Pourcentage	100 %	29 %	43 %	14 %	14 %

Conclusion

La direction a réussi à appliquer deux des six recommandations qui sont toujours applicables.

On n'a pas encore commencé à suivre une recommandation se rapportant à l'approbation à délivrer avant d'apporter des modifications aux champs du fichier principal des fournisseurs. La Ville n'a pas configuré les champs confidentiels du fichier principal des fournisseurs dans SAP parce qu'on s'attend à mettre en œuvre, en 2020, une nouvelle solution Source de paiement pour donner suite à cette recommandation. C'est pourquoi on risque toujours d'effectuer des paiements avant que les champs confidentiels du fichier principal des fournisseurs soient revus et approuvés en bonne et due forme.

Voici les trois recommandations appliquées en partie : on a évalué la question de la conservation des documents faisant état des conflits dans la DT et on a réglé les problèmes avant de donner des droits d'accès supérieurs au système; on a prévu des

processus permettant de suivre les pénalités pour frais de retard et d'en rendre compte; enfin, on a automatisé la surveillance des rabais potentiels en fonction des dates de réception des factures. Le lecteur trouvera ci-après de plus amples renseignements sur l'état de la mise en œuvre de chaque recommandation appliquée partiellement.

Dans la vérification menée à l'origine, on a constaté que bien que le processus de dépistage des conflits potentiels dans la DT existe et que la documentation soit disponible, aucune pièce justificative n'a pu être déposée pour démontrer que le processus était appliqué uniformément. C'est pourquoi les vérificateurs ont recommandé que la Ville conserve des pièces justificatives qui démontrent que dans les cas où l'on attribue des droits d'accès supérieurs au système, les conflits dans la DT ont été évalués et réglés avant l'approbation des factures. Nos travaux de suivi ont permis de constater que bien que l'obligation de conserver des documents ait été officialisée, ces documents ne sont pas conservés uniformément dans tous les cas où l'on attribue des droits d'accès supérieurs au système.

À l'issue de la vérification menée à l'origine, on a également recommandé à la direction d'instituer un processus permettant de suivre les pénalités pour retard acquittées en raison des processus de l'UCC et d'en rendre compte. Nos travaux de suivi ont permis de confirmer que bien que l'UCC ait effectivement prévu un compte de frais désigné dans MarkView pour permettre de suivre les pénalités et intérêts pour retard, c'est à l'utilisateur opérationnel qu'il appartient de prendre connaissance de la pénalité pour retard dans les factures et de la coder dans le compte de frais. L'UCC n'a pas pu fournir de pièce justificative faisant état des modalités selon lesquelles les utilisateurs opérationnels recevaient des avis à propos de ce compte et de l'obligation qui leur est imposée de coder dans ce compte les pénalités ou les frais de retard, ni des cas dans lesquels ils reçoivent ces avis et doivent coder ces pénalités ou frais.

Enfin, dans la vérification menée à l'origine, on a recommandé que la Ville profite de la technologie existante pour assurer l'efficacité et l'efficacités des opérations de l'UCC, notamment en automatisant la surveillance des rabais potentiels d'après la date de réception des factures. On a reporté les améliorations à apporter au système pour la surveillance et l'analytique, et ces améliorations seront apportées dans le cadre de la nouvelle solution Source de paiement.

L'une des sept recommandations exprimées à l'origine n'est plus applicable. Quand on a fait l'analyse d'une solution, on a constaté que les systèmes actuels ne permettent pas d'établir des rapports plus précis sur les résultats des unités opérationnelles.

Le Bureau du vérificateur général s'est réuni avec la direction à propos des recommandations partiellement appliquées, et la direction a fait savoir qu'elle a l'intention d'appliquer les recommandations en suspens.

Recommandations et réponses

Recommandation

Que l'UCC officialise l'obligation et les mesures destinées à mener, deux fois par an, l'« analyse des factures en double » dans le texte d'une procédure.

Réponse de la direction

La direction est d'accord avec cette recommandation.

Les mesures à prendre pour mener, deux fois par an, l'analyse des factures en double sera décrite dans une procédure formelle d'ici le troisième trimestre de 2019.

Recommandation

Avant d'apporter cette modification dans l'affectation des transactions effectuées par cartes d'achat, l'UCC devrait porter, à l'attention des utilisateurs des cartes d'achat, le risque de factures en double et leur obligation de mettre en œuvre un processus permettant de s'assurer que les paiements traités dans MarkView n'ont pas déjà été effectués grâce à une carte d'achat.

Réponse de la direction

La direction est d'accord avec cette recommandation.

Les Services de l'approvisionnement reproduiront un rappel dans les relevés mensuels adressés à tous les titulaires de cartes pour attirer leur attention sur le risque de factures en double et sur leur obligation de mettre en œuvre un processus pour s'assurer que les paiements traités dans MarkView n'ont pas déjà été effectués grâce à une carte d'achat. Cette mesure sera prise au premier trimestre de 2019.

Remerciements

Nous tenons à remercier la direction pour la collaboration et l'assistance accordées à l'équipe de vérification.

Suivi de la vérification de 2015 du Projet de lecture automatisée des compteurs d'eau

Le suivi de la vérification de 2015 du Projet de lecture automatisée des compteurs d'eau (LACE) faisait partie du Plan de vérification 2018 du Bureau du vérificateur général.

Voici les principales constatations qui ont été faites dans le cadre de la mission de vérification menée à l'origine en 2015 :

- Le projet de lecture automatisée des compteurs d'eau s'appuyait sur une structure de gouvernance ayant permis la réalisation et la gestion économiques et efficaces du projet. Toutefois, aucun comité directeur n'a été formé, et c'est seulement plus de trois ans après la fin du projet qu'un responsable opérationnel unique a été désigné.
 - Le projet de lecture automatisée des compteurs d'eau s'appuyait sur une structure de gouvernance ayant permis la réalisation et la gestion économiques et efficaces du projet. Toutefois, aucun comité directeur n'a été formé, et c'est seulement plus de trois ans après la fin du projet qu'un responsable opérationnel unique a été désigné.
- Le projet a été bien planifié et mis en œuvre et a été géré dans un souci d'économie et d'efficacité.
 - Les 195 000 modules prévus à l'origine dans la portée des travaux ont été installés avec succès, en tenant compte des 10 000 installations retranchées à l'origine dans la portée des travaux, et le projet a continué de se dérouler dans le respect du calendrier et du budget.
- La plupart des objectifs, des économies attendues, des objectifs stratégiques et des améliorations à apporter aux services dans le cadre de ce projet l'ont été avec succès. Toutefois, les économies de coûts et la réalisation des objectifs stratégiques du projet n'ont pas fait l'objet d'un suivi ni d'un rapport complet.
 - Bien que certaines économies aient été réalisées en réduisant l'effectif, les économies de coûts réalisées grâce à la mise en œuvre de l'infrastructure de comptage avancée (ICA) n'ont pas été comptabilisées dans un rapport.

Suivi de la vérification de 2015 du
Projet de lecture automatisée des compteurs d'eau

Tableau 1 : Sommaire de l'état de la mise en œuvre des recommandations

Recommandations	Total	Achevées	En cours	À venir	Ne s'appliquent plus
Nombre	4	4	0	0	0
Pourcentage	100 %	100 %	0 %	0 %	0 %

Conclusion

La direction a accompli d'énormes progrès dans la mise en œuvre des quatre recommandations qui lui ont été adressées. Nous suggérons que désormais, la direction fasse état de prix variables et de prix fixes dans les contrats pertinents afin d'encourager les entrepreneurs à s'acquitter de leurs fonctions tout en respectant les objectifs de la Ville.

Remerciements

Nous tenons à remercier la direction pour la collaboration et l'assistance accordées à l'équipe de vérification.

Suivi de la vérification de 2014 des opérations hivernales : planification de la capacité et indicateurs de rendement

Le suivi de la vérification de 2014 des opérations hivernales : planification de la capacité et indicateurs de rendement faisait partie du Plan de vérification 2017 du Bureau du vérificateur général.

Voici les principaux constats de la vérification originelle de 2014 :

1. Il n'y avait pas de processus consigné par écrit qui tienne compte des besoins en capacité des ressources pour les opérations hivernales dans le cycle annuel de planification ou de budgétisation.
2. Les Normes de qualité de l'entretien (NQE) existantes relativement au déneigement et au déglçage ont été adoptées en mai 2003. Depuis, les normes et leurs répercussions financières n'ont pas été revues et évaluées systématiquement.
3. La répartition des travaux entre les fournisseurs de services internes et les fournisseurs de services externes se fondait essentiellement sur d'anciens systèmes qui existaient au moment de la fusion. Depuis, il n'y a pas eu d'examen pour déterminer la répartition optimale des travaux entre les fournisseurs de services internes et les fournisseurs de services externes.
4. Le Service des travaux publics n'avait pas de processus consigné par écrit pour recenser les gains potentiels d'efficacité opérationnelle.
5. Dans les cas où il n'était pas nécessaire d'épandre des abrasifs ou de déneiger, le personnel était affecté à différentes tâches. Il n'existait pas de liste imprimée des tâches à accomplir en priorité, et les tâches auraient pu être assurées plus économiquement en faisant appel à des entreprises commerciales.
6. Tous les véhicules de déneigement appartenant à la Ville et à des sous-traitants étaient équipés de deux systèmes de positionnement global (GPS) propres aux tâches. La direction n'avait pas déterminé si les avantages que devaient apporter ces investissements dans la technologie avaient été réalisés.

Suivi de la vérification de 2014 des opérations hivernales :
Planification de la capacité et indicateurs de rendement

7. La Ville avait un plan de communication détaillé pour les interdictions de stationner la nuit. La direction était d'avis qu'il ne serait pas pratique de mettre en œuvre une « interdiction en rotation » pour les interdictions de stationner la nuit relativement aux travaux de déneigement comme on le fait dans certaines municipalités.
8. Les rapports mensuels sur les écarts comprenaient des indicateurs appropriés et pertinents, par exemple la comparaison des coûts budgétés par rapport aux coûts réels et détaillés par catégorie. On aurait pu améliorer les rapports grâce à des commentaires sur les facteurs de coûts liés au rendement.
9. Les principaux indicateurs de rendement (PIR) utilisés pour évaluer les opérations hivernales correspondaient aux normes approuvées par le Conseil et précisées dans les NQE. On n'établissait pas de rapport à intervalles réguliers à l'intention de la direction, du Comité ou du Conseil municipal. Les rapports sur les PIR ne comprenaient pas l'information disponible dans le rapport de l'Initiative d'analyse comparative des services municipaux (IACSM) de l'Ontario.
10. Les examens menés par les superviseurs pour les activités de déneigement étaient essentiellement déstructurés et fondés sur les résultats techniques. Aucun document ne venait attester que les NQE étaient appliquées uniformément sur l'ensemble du territoire de la Ville ou que ces normes étaient respectées rigoureusement ou largement.
11. La Procédure opérationnelle normalisée pour les livraisons de sel permettait d'accepter des livraisons très variables et ne précisait pas le nombre de pesées aléatoires qui devaient être effectuées. On n'exerçait aucune surveillance pour s'assurer que les balances portables étaient utilisées dans toutes les cours pendant toute la saison hivernale et pour veiller à ce que les entrepreneurs ne soient pas prévenus. Les quantités de sel restant au printemps de 2012, de 2013 et de 2014 étaient inférieures aux quantités en stock selon le système SAP.

Suivi de la vérification de 2014 des opérations hivernales :
Planification de la capacité et indicateurs de rendement

12. En date de juin 2015, 96 % des travailleurs et 95 % des superviseurs de la Direction du service des routes avaient suivi la formation de sensibilisation à la santé et à la sécurité au travail. Le Service des travaux publics était en train d'évaluer les risques des activités professionnelles dans le cadre des opérations hivernales pour le recensement des dangers et l'évaluation des risques (RDER).

Tableau 1 : Sommaire de l'état de la mise en œuvre des recommandations

Recommandations	Total	Achevées	En cours	À venir	Ne s'appliquent plus
Nombre	20	17	3	0	0
Pourcentage	100 %	85 %	15 %	0 %	0 %

Conclusion

La direction a accompli des progrès satisfaisant en appliquant 17 des 20 recommandations.

La direction a aussi accompli des progrès significatifs en mettant en œuvre partiellement trois recommandations. Elle devrait continuer d'évaluer en permanence les coûts, les avantages et les gains d'efficacité de l'externalisation des services afin d'assurer la répartition optimale des ressources internes et des ressources externes. Enfin, le tableau de bord du Service des routes, qui vise à améliorer les rapports financiers et les rapports sur les PIR, devrait être mis en œuvre d'ici la fin du deuxième trimestre de 2019.

Remerciements

Nous tenons à remercier la direction pour la collaboration et l'assistance accordées à l'équipe de vérification.

Suivi de la vérification de 2015 de la gouvernance des technologies de l'information

Le Suivi de la vérification de 2015 de la gouvernance des technologies de l'information faisait partie du Plan de vérification 2018 du Bureau du vérificateur général.

La Direction générale des services de technologie de l'information (DGSTI) de la Ville d'Ottawa (la « Ville ») est essentiellement chargée de déployer et de maintenir les ressources de TI servant à assurer les services de la Ville à l'intention des résidents, des entreprises et des visiteurs d'Ottawa. En 2013, le STI avait un budget de fonctionnement net de 52,1 millions de dollars et comptait 352 équivalents temps plein. Son budget des immobilisations était de 11,5 millions de dollars. La structure de gouvernance de la Ville d'Ottawa, comme celle d'autres villes d'Ontario, facilite le processus législatif. Elle est en effet composée de plusieurs organes différents, quoique liés, soit le Conseil municipal, les comités permanents et consultatifs et les agences, offices, commissions et conseils indépendants, ainsi que d'outils de réglementation qui régissent ces comités, dont le *Règlement de procédure*, le *Règlement municipal sur la délégation de pouvoirs* et le *Règlement sur l'affichage public*.

La structure de gouvernance de la Ville est conçue pour permettre à la communauté de participer de manière directe et officielle au processus décisionnel au moyen de présentations des membres citoyens qui siègent aux comités consultatifs et en faisant des présentations devant les élus aux comités permanents. Elle favorise aussi le travail législatif et gouvernemental des représentants élus par le biais des réunions des comités permanents et du Conseil municipal. La gouvernance des TI est un sous-élément de la structure de gouvernance générale de la Ville.

La vérification menée à l'origine a permis de cerner les points à améliorer, qui ont été classés sous cinq thèmes prépondérants :

1. **Structures organisationnelles et de gouvernance** : L'Institut des vérificateurs internes affirme que des structures organisationnelles claires, la nature opérationnelle de leurs composantes et la façon dont elles communiquent entre elles, et les protocoles de reddition de comptes sont importants afin que les services de TI puissent offrir les types et niveaux de service nécessaires pour que l'entreprise atteigne ses objectifs.

Voici les constatations précises faites dans le cadre de la vérification menée à l'origine :

- manque de documents explicites sur la façon dont le STI soutient la Ville dans l'atteinte de ses grands objectifs;
- risque que les points clés ne soient pas abordés dans les réunions de l'équipe de gestion de la technologie de l'information municipale (ÉGTIM¹), puisque ces réunions ne se déroulent pas selon un ordre du jour établi en bonne et due forme;
- le Comité de la gouvernance des TI² n'a pas d'attributions officielles; il n'y a donc aucun document officiel qui décrit son but et sa structure;
- Les accords de contribution individuelle³ (ACI) ne contiennent pas assez d'objectifs mesurables (soit les projets mis en œuvre avec succès dans le respect des délais ou du budget). On considère que ces objectifs sont de bonnes pratiques pour renforcer les responsabilités du personnel du STI, y compris du chef de l'information.

2. **Soutien et leadership de la direction** : Une voix forte au gouvernail et le leadership de la direction jouent un rôle important dans l'alignement des TI sur les objectifs organisationnels généraux. Cela signifie qu'il y a une vision sûre chez les cadres supérieurs et membres de la direction quant à l'importance stratégique et potentielle des services de TI. Il y a plusieurs éléments qui permettent un leadership et un soutien de la direction forts et qu'on s'attendait à trouver au cours de la vérification.

Voici les constatations précises faites dans le cadre de la vérification menée à l'origine :

¹ L'ÉGTIM a été dissoute dans la foulée de la mission de vérification menée à l'origine.

² Le Comité de la gouvernance de la TI a été dissous dans la foulée de la mission de vérification menée à l'origine.

³ Le 5 décembre 2017, la Ville a déclaré, dans une note de service destinée aux employés municipaux, que « Comme nous l'avons annoncé l'an dernier à l'occasion des forums des gestionnaires municipaux, la Ville a mis fin au processus officiel de l'ACI pour adopter une pratique dynamique qui mise sur des dialogues de mise au point qui se tiennent à intervalles réguliers entre les gestionnaires et superviseurs et les employés sur l'ensemble de l'année ». Ce nouveau processus s'appelle la « gestion du rendement ».

Suivi de la vérification de 2015
de la gouvernance des technologies de l'information

- taux de roulement élevé dans la fonction de chef de l'information (CI);
- manque de communication à propos du rôle des STI dans la réalisation des objectifs stratégiques de la Ville;
- absence d'indicateurs de rendement officiels liés à la valeur stratégique du STI.

3. **Planification stratégique et opérationnelle** : Un plan stratégique, qui établit les liens de dépendance organisationnelle par rapport aux TI de même que le rôle du STI dans la concrétisation des objectifs stratégiques de l'organisation, est une composante fondamentale d'une gouvernance des TI efficace. Des pratiques novatrices mettent aussi l'accent sur le besoin d'aligner le plan opérationnel tactique du STI sur le *Plan stratégique de la Ville*.

Voici les constatations précises faites dans le cadre de la vérification menée à l'origine :

- l'absence de liens explicites et d'une terminologie commune dans le Plan stratégique et les projets de TI décrits dans la Feuille de route technologique;
- le Plan stratégique ne définit pas clairement le rôle et les responsabilités du STI dans l'atteinte des objectifs stratégiques et ne précise pas non plus les liens de dépendance de la Ville par rapport aux TI;
- nous n'avons pas relevé d'autres exemples dans lesquels la Ville a tenu compte de la capacité actuelle et prévue en TI au sein des STI;
- utilisation insuffisante des indicateurs de rendement et des outils d'évaluation connexes — les indicateurs existants se sont avérés insuffisants, car ils mettent l'accent seulement sur les aspects opérationnels fondamentaux des services de TI (p. ex. temps d'arrêt) et les indicateurs de base liés aux projets de TI.

4. **Prestation et évaluation des services** : Comme on le précise dans le GTAG 17⁴, un cadre de gestion du rendement efficace englobe les données quantitatives et qualitatives nécessaires à une évaluation, à une analyse et à une transparence proactives de sorte à assurer une saine gouvernance des TI.

⁴ Institute of Internal Auditors - Global Technology Audit Guide (GTAG) 17: Auditing IT Governance - <https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/pages/gtag17.aspx>

Suivi de la vérification de 2015
de la gouvernance des technologies de l'information

Voici les constatations précises faites dans le cadre de la vérification menée à l'origine :

- les intervenants ne comprennent pas trop en quoi les coûts des TI s'inscrivent dans l'atteinte des objectifs stratégiques de la Ville;
- le STI n'évalue pas efficacement sa valeur, tant en ce qui a trait à la contribution aux objectifs stratégiques qu'aux avantages opérationnels associés aux projets de TI.

5. **Organisation des TI et gestion des risques** : Pendant l'évaluation des pratiques de gestion des risques de l'organisation en matière de TI, on s'attendait à définir trois éléments clés. D'abord, on s'attendait à ce que des politiques, procédures et mesures de contrôle standard en matière de matériel, de logiciels et d'approvisionnement en services soient en place. Ensuite, on s'attendait à une gestion des risques efficace par rapport aux besoins de la Ville et à ses exigences en matière de sécurité et de conformité. Enfin, le GTAG 17 précise que les données doivent être normalisées et faciles à partager dans les applications et les infrastructures des TI.

Voici les constatations précises faites dans le cadre de la vérification menée à l'origine :

- absence de documents étayant l'établissement et l'évaluation (probabilité et incidence) des risques au sein du STI;
- rien dans la politique sur la gestion des risques du STI n'indique la façon de communiquer les risques prioritaires en matière de TI au comité responsable de la Ville. De plus, la communication descendante des risques organisationnels au STI n'est pas claire, le tout se traduisant par un alignement flou des risques du STI sur les risques organisationnels globaux.

Pour tenir compte des points à améliorer évoqués ci-dessus, la Vérification de la gouvernance des TI menée à l'origine a permis de formuler neuf recommandations à l'intention de la Ville d'Ottawa. Le Suivi de la vérification 2015 de la gouvernance des technologies de l'information a porté sur l'évaluation de l'avancement de chacune des recommandations, dont le tableau 1 ci-après donne un aperçu. Le lecteur trouvera dans le rapport détaillé les détails de cette évaluation.

Suivi de la vérification de 2015
de la gouvernance des technologies de l'information

Tableau 1 : Sommaire de l'état de mise en œuvre des recommandations

Recommandations	Total	Achevées	En cours	Impossibles à évaluer
Nombre	9	4	5	0
Pourcentage	100 %	44 %	56 %	0 %

Voici les recommandations en cours d'application :

- *Que l'Équipe de gestion de la technologie de l'information municipale puisse compter sur des ordres du jour officiels et le Comité de la gouvernance des TI, dans la mesure où il continue de jouer un rôle officiel, de même que sur des attributions officielles précisant le but et la structure de l'Équipe.* L'ÉGTIM et le Comité de la gouvernance des TI ont été dissous dans la foulée de la mission de vérification menée à l'origine et ont été remplacés respectivement par le Comité de la technologie opérationnelle et le Comité de la direction. Nous constatons que les comités de la gouvernance ont été actualisés depuis la mission de vérification menée à l'origine et qu'il existe des mandats en bonne et due forme et des programmes permanents pour les nouveaux comités; toutefois, nous avons noté que les politiques et les processus de gestion des risques de TI actuels de la Ville manquent de cohérence à propos des rôles, des responsabilités et des pouvoirs liés aux approbations à délivrer pour les exemptions et les exceptions au titre des procédures normalisées (ce qui influe sur l'efficacité des mécanismes de gouvernance).
- *Que désormais, le processus d'établissement des objectifs de l'ACI du chef de l'information soit revu de sorte que ces objectifs soient mesurables.* Nous avons noté que le chef de l'information a mis au point son plus récent ACI et ses plus récents objectifs de rendement, en s'inspirant des objectifs et des résultats clés (ORC) décrits; toutefois, on pourrait tenir compte d'autres objectifs dans l'évaluation du rendement du chef de l'information, par exemple la résolution de problèmes précis relatifs aux ORC dans le plan de travail stratégique de la DGSTI correspondant aux recommandations importantes qui découlent des missions de vérification menées à l'origine sur la gouvernance des TI, sur la gestion des

Suivi de la vérification de 2015
de la gouvernance des technologies de l'information

risques et sur l'accès à distance aux TI (et qui sont décrites dans la section 8 du plan de travail stratégique des STI)

- *Que la direction accélère le processus de recrutement d'un chef de l'information qualifié et chevronné. De plus, qu'elle examine et confirme les attentes et les pratiques connexes applicables au chef de l'information afin d'assurer leur alignement sur les pratiques exemplaires, selon lesquelles les services de TI sont vus comme un moteur stratégique, puis habilités et soutenus en ce sens.* Nous avons noté, dans le rapport de vérification originel (mars 2015) que « Le roulement au poste de chef de l'information est important. Avec le départ en décembre 2013 du nouveau chef de l'information, huit personnes ont occupé le poste depuis mars 2004, que ce soit à titre officiel ou provisoire, dont cinq depuis juin 2012 ».⁵ La description du travail du chef de l'information n'obligeait pas le candidat à être expressément un « chef de l'information chevronné », et nous avons noté que le chef de l'information s'est par la suite démis de ses fonctions à la Ville en janvier 2019.
- *Que la direction élabore un plan de relève efficace pour le poste de chef de l'information afin de le mettre en œuvre une fois le titulaire choisi.* Nous avons noté qu'il n'existait pas, pour le poste du chef de l'information, de plan de relève consigné par écrit.
- *Que la politique sur la gestion des risques du STI comprenne des éléments indiquant la façon de communiquer les risques prioritaires en matière de TI au comité de gestion des risques de la Ville⁶. De plus, le STI devrait collaborer avec le personnel de la Ville à l'élaboration d'un cadre régissant les attentes en matière de communication descendante des risques organisationnels au STI. Le STI devrait aussi créer ou obtenir des documents officiels qui décrivent l'établissement et l'évaluation des risques en TI au sein du service.* Nous constatons que les comités de la gouvernance ont été actualisés depuis la mission de vérification menée à l'origine et qu'il existe des mandats en bonne et due forme et des programmes permanents pour les nouveaux comités; toutefois, nous avons noté que les politiques et les processus de gestion des risques de TI

⁵ Ville d'Ottawa, Bureau du vérificateur général, Vérification de la gouvernance des TI – mars 2015, page 7.

⁶ Le Comité de gestion des risques de la Ville a été dissous dans la foulée de la mission de vérification menée à l'origine.

actuels de la Ville manquent de cohérence à propos des rôles, des responsabilités et des pouvoirs liés aux approbations à délivrer pour les exemptions et les exceptions au titre des procédures normalisées.

Conclusion

La direction a démontré qu'elle avait progressé dans l'application des recommandations découlant de la vérification de la gouvernance des technologies de l'information, le Bureau du vérificateur général (BVG) a noté qu'il faut toujours prendre des mesures d'atténuation dans un certain nombre de secteurs essentiels. En particulier, on a évalué que cinq des neuf recommandations n'avaient été appliquées qu'en partie.

Nous avons noté que les STI ont établi un lien concret entre les services de TI et les grands objectifs de la Ville. Ils l'ont fait grâce à deux initiatives : un nouveau processus de prise en charge des projets et un plan de travail stratégique des STI, qui instituent un cadre pour la planification et le déroulement des activités des STI de 2018 à 2020. Nous avons constaté que ces deux initiatives suivent des orientations axées sur la clientèle et qui établissent des liens entre les besoins opérationnels et les services des STI. Nous avons noté qu'on avait cessé d'utiliser la fiche de notation des STI, qui se servent d'un tableau de bord des clients pour afficher des indicateurs, notamment les demandes de services par direction générale, les projets pris en charge et les activités des directions générales, et que ce tableau de bord se situe dans une phase pilote avant d'être déployé à plus grande échelle. On a aussi adopté des indicateurs correspondant aux objectifs et aux résultats clés, et nous avons relevé des pièces justificatives démontrant que ces indicateurs ont été notés et surveillés chaque mois, comme le suggère le Plan de travail stratégique des STI dans la section 14.1.2.

Nous reconnaissons que les comités de gouvernance ont été actualisés depuis la mission de vérification menée à l'origine et qu'on a mis en place des mandats officiels et des programmes permanents; toutefois, nous avons relevé certaines incohérences dans les politiques et les processus de gestion des risques de TI actuels de la Ville à propos des rôles, des responsabilités et des pouvoirs se rapportant aux approbations à délivrer pour les exemptions et les exceptions au titre des procédures normalisées.

Nous avons noté que la Ville doit à nouveau relever le défi qui consiste à recruter et à établir un nouveau chef de l'information. D'ici là, l'efficacité de la gouvernance des TI risque plus d'être réduite considérablement. En outre, les STI n'ont pas réussi à donner

Suivi de la vérification de 2015
de la gouvernance des technologies de l'information

suite comme il se doit, en temps utiles depuis 2015, à un certain nombre de constatations des vérificateurs, [REDACTED].

Remerciements

Nous tenons à remercier la direction pour la collaboration et l'assistance accordées à l'équipe de vérification.

Suivi de la vérification de 2015 de la gestion des risques liés aux technologies de l'information

Le suivi de la vérification de 2015 de la gestion des risques liés aux technologies de l'information faisait partie du Plan de vérification 2018 du Bureau du vérificateur général.

Les solutions et innovations fondées sur les TI permettent de réaliser les divers objectifs stratégiques et opérationnels dans tous les services de la Ville. Des solutions novatrices sont sans cesse créées, et l'on s'attend à ce que l'importance des technologies continue d'augmenter très rapidement. Toutefois, même si les TI peuvent favoriser grandement l'atteinte des objectifs stratégiques de la Ville, il faut tenir compte des nombreux risques, connus et inconnus, qui doivent être gérés au niveau le plus élevé.

Une administration aussi importante et complexe que la Ville d'Ottawa s'expose à des risques liés aux TI d'une ampleur considérable. L'utilisation des TI dans les différentes activités municipales entraîne un risque inhérent lorsqu'il s'agit d'assurer l'efficacité opérationnelle et administrative, de protéger des actifs de valeur et de nature délicate, de respecter les normes ou de se conformer à des exigences stratégiques et opérationnelles. Ainsi, bien que l'utilisation des TI comporte évidemment des risques de nature technique, ce sont les gestionnaires des différents services qui sont les principaux intervenants dans la gestion des risques liés aux TI.

Un certain nombre de politiques, de processus et de pratiques encadrent la gestion des risques liés aux TI, autant à l'échelle de l'organisation qu'à une échelle beaucoup plus restreinte (p. ex. au niveau des projets de TI ou de la réaction à un incident isolé). Les risques liés aux TI à l'échelle de l'organisation sont indiqués explicitement dans le cadre de gestion. Bien que le Service de technologie de l'information (STI) soit le plus à risque, il a été déterminé en 2014 que 65 % des services présentent des risques liés aux TI.

Les STI jouent un rôle important dans la gestion des risques liés aux TI sur le plan des projets et des systèmes. En plus d'offrir des séances de formation et de sensibilisation, les STI sont chargés d'élaborer des politiques et des lignes directrices encadrant la gestion des risques liés aux TI.

Suivi de la vérification de 2015
de la gestion des risques liés aux technologies de l'information

Les STI sont officiellement chargés de gérer les risques liés aux TI en général, mais des équipes autonomes gèrent des applications et des systèmes indépendants (bien qu'ils soient souvent connectés au moins partiellement au reste du réseau) dans certains services et directions, notamment le Service de transport en commun, la Direction de la circulation routière, la Direction des services de gestion de l'eau potable et la Direction de la gestion des eaux usées.

La vérification menée à l'origine a permis de cerner les points à améliorer, qui ont été classés dans trois catégories d'objectifs :

1. Évaluer l'efficacité de la gouvernance municipale associée à la gestion des risques liés aux TI

Voici les constatations précises faites dans le cadre de la vérification menée à l'origine :

- L'absence d'un cadre de gestion des risques liés aux TI comportant une section consacrée à la gouvernance et qui préciserait de manière claire et cohérente les responsabilités des cadres et les gestionnaires municipaux;
- La méthode décentralisée d'établissement des priorités, de sélection et de financement des initiatives de TI pourrait donner lieu à des projets approuvés qui ne cadrent pas avec les priorités de la Ville, et l'on a recensé des risques importants permettant de conclure que des risques de TI absolument prioritaires ne sont pas pris en compte suffisamment tôt dans les cas où le financement n'est pas mis rapidement à la disposition du responsable opérationnel;
- La capacité de l'Équipe de gestion de la TI municipale (EGTIM¹) à s'acquitter de sa responsabilité de recommander un plan municipal en matière de TI qui reflète les priorités municipales fondées sur les risques liés aux TI est limitée par le modèle existant de financement des projets de TI de même que par la capacité actuelle de la Ville à cerner et à prioriser les risques globaux liés aux TI;

¹ L'ÉGTIM a été démantelée dans la foulée de la mission de vérification menée à l'origine.

Suivi de la vérification de 2015
de la gestion des risques liés aux technologies de l'information

- La capacité du chef de l'information à gérer et à influencer les ressources de TI de la Ville est limitée puisque le personnel responsable des TI dans les différents services et organismes (p. ex. Santé publique Ottawa, Service de transport en commun, Services d'eau, Direction de la gestion des eaux usées) n'est pas techniquement soumis à son autorité et que la hiérarchie n'est pas toujours clairement établie, et que les pouvoirs et les responsabilités du chef de l'information en ce qui a trait aux risques liés aux TI à l'échelle municipale ne sont pas définis rigoureusement.

2. **Déterminer si les politiques, les pratiques et les procédures municipales définies par le cadre de gestion des risques liés aux TI sont adéquates et conformes au cadre de GAR.**

Voici les constatations précises faites dans le cadre de la vérification menée à l'origine :

- Il n'y a pas de cadre complet de gestion des risques liés aux TI qui permettrait de faire le lien entre la GAR et la gestion des risques à petite échelle.
- La documentation est très lacunaire en ce qui a trait à la détection, à l'évaluation et à l'atténuation des risques liés aux TI. Par ailleurs, l'efficacité du cadre de gestion des risques liés aux TI existant est réduite en raison de l'absence de cadre de gestion des risques liés aux TI approuvé et suffisamment documenté et comprenant les politiques et procédures requises, l'insuffisance des processus municipaux de détection et d'évaluation des risques liés aux TI, les lacunes des mécanismes de vérification pour l'évaluation des mesures correctives proposées, la formation insuffisante du personnel du STI et des employés en dehors du STI, spécialistes des TI ou non, responsables de l'évaluation des risques dans les autres services, le manque de documentation spécialisée sur laquelle pourraient s'appuyer les gestionnaires, les lacunes du Plan de technologie opérationnelle, qui se concentre surtout sur l'atténuation des risques majeurs, et l'inadéquation des échéanciers, des dépenses et des sources de financement connexes.

Suivi de la vérification de 2015
de la gestion des risques liés aux technologies de l'information

- Étant donné les lacunes de nombreux services en matière de gestion des risques liés aux TI de même que la portée et la nature technique des risques liés aux TI, les procédures et les orientations de la Ville et des différents services ne suffisent pas à garantir que la détection, l'évaluation, le signalement, l'atténuation et le suivi des plus importants risques liés aux TI se fassent de manière cohérente et appropriée et suffisamment tôt. De plus, les problèmes et les priorités en matière de TI qui touchent les objectifs globaux de la Ville ne parviennent pas nécessairement aux gestionnaires.

3. Déterminer si les politiques, les pratiques et les procédures municipales définies par le cadre de gestion des risques liés aux TI concourent effectivement au repérage, à l'évaluation, à l'atténuation et au contrôle des risques liés aux TI.

Voici les constatations précises faites dans le cadre de la vérification menée à l'origine :

- La Ville ne possède ni la culture d'entreprise ni les moyens requis pour adopter une approche globale de la gestion des risques liés aux TI;
- Les données actuelles n'ont pas nécessairement fait l'objet d'analyses, de vérifications et d'examen suffisants par des personnes ayant les compétences nécessaires et appropriées;
- Certains problèmes liés aux TI pourraient ne pas être détectés ou évalués, et par conséquent signalés (sensibilisation) et atténués (planification et financement);
- Il est difficile de savoir si tous les risques liés à des questions comme l'infrastructure vieillissante, le stockage des données et la capacité du réseau ont été détectés;
- Il n'y a pas toujours de corrélation entre la détection d'un risque majeur et l'allocation des ressources requises pour l'atténuer.

Pour corriger les points ci-dessus, la vérification menée à l'origine pour la gestion des risques liés aux technologies de l'information a permis de formuler huit recommandations à mettre en œuvre par la Ville d'Ottawa. Le suivi de la vérification 2015 de la gestion des risques liés aux technologies de l'information a permis d'évaluer l'avancement de l'application de chaque recommandation, dont les résultats sont

Suivi de la vérification de 2015
de la gestion des risques liés aux technologies de l'information

résumés dans le tableau 1 ci-après. Les détails de cette évaluation sont compris dans le rapport détaillé.

Tableau 2 : Sommaire de l'état de mise en œuvre des recommandations

Recommandations	Total	Achevées	En cours	Impossibles à évaluer
Nombre	8	0	7	1
Pourcentage	100 %	0 %	88 %	12 %

Voici les recommandations en cours d'application :

- *Que le directeur municipal crée une section consacrée à la gouvernance dans un cadre de gestion des risques liés aux TI qui :*
 - *s'harmonise avec le cadre de GAR et comprend une section consacrée à la gouvernance, qui vient promouvoir une culture évoluée de maîtrise des risques intégrée dans un cadre de GRTI grâce à une série de politiques et de processus auxiliaires.* Nous avons observé que les politiques de gouvernance ont été harmonisées avec les objectifs du cadre de GAR, alors que le processus annuel de validation des risques, qui est un processus essentiel du cadre de GRTI, a été mis au point au moment de la vérification.
 - *définit clairement les rôles, les responsabilités et les pouvoirs des cadres supérieurs et des gestionnaires de la Ville, afin de désigner clairement ceux qui sont responsables, redevables, consultés et informés pour assurer l'efficacité de la GRTI.* Les rôles et les responsabilités ont été plus clairement définis lorsqu'on a adopté le cadre de GRTI; toutefois, nous avons noté que les politiques et les processus actuels de la Ville pour la gestion des risques de TI manquent d'uniformité en ce qui concerne les approbations à délivrer pour les exemptions ou les exceptions au titre des procédures normalisées (ce qui influe sur les rôles, les responsabilités, de même que sur la gouvernance et l'encadrement des risques de TI). Nous avons également constaté que certaines personnes-ressources des Services de soutien aux activités n'ont pas les connaissances technologiques ni la formation rigoureuse sur les risques des TI pour pouvoir recenser les risques potentiels de TI et participer à l'évaluation des risques de TI;

Suivi de la vérification de 2015
de la gestion des risques liés aux technologies de l'information

- *établit clairement le fondement d'une culture générale des risques, ainsi que des lignes directrices sur la tolérance au risque et l'appétence au risque.* La Ville a apporté des améliorations en établissant des lignes directrices sur l'appétence et la tolérance au risque, notamment en dressant la liste de 53 risques pour les secteurs d'activité et un processus plus rigoureux pour les exemptions au titre des risques; on met actuellement au point un processus annuel de validation des risques.
- *s'assure que l'on tient compte de toutes les stratégies d'atténuation des risques dont les seuils de tolérance admissibles sont dépassés pour les intégrer dans le plan municipal annuel de TI d'après l'importance des risques ou les priorités, qu'on ait déjà approuvé ou non le financement voulu.* À l'heure actuelle, on prend les décisions dans les stratégies d'atténuation des risques dans le cadre du budget annuel, et ces décisions sont rarement adoptées hors de cette structure. Nous avons noté que le plan des STI porte essentiellement sur les dépenses en immobilisations, ainsi que sur l'élaboration et la mise à jour des processus clés, et que le financement est lié aux objectifs et aux résultats clés. Toutefois, les modèles de financement de la Ville d'Ottawa n'ont pas permis de maîtriser les risques opérationnels de TI se rapportant aux constatations découlant de la Vérification de 2015 de la gestion des incidents de sécurité des TI et des interventions connexes [REDACTED], ce qui indique que le financement des risques opérationnels de TI n'a peut-être pas suivi le rythme voulu.
- *Que le directeur municipal et la trésorière municipale évaluent les dépenses liées aux TI et envisagent des modèles de financement qui permettraient que les fonds disponibles soient consacrés à atténuer les risques prioritaires à l'échelle de la Ville, et ce, afin de réaliser des économies à long terme en ciblant mieux les dépenses.* La Ville a adopté de nouveaux modèles de financement, afin de permettre de financer les risques de TI inadmissibles. Toutefois, les modèles de financement de la Ville d'Ottawa n'ont pas permis de maîtriser les risques opérationnels des TI se rapportant aux constatations découlant de la Vérification de 2015 de la gestion des incidents de sécurité des TI et des interventions connexes [REDACTED], ce qui indique que le financement des risques opérationnels de TI n'a peut-être pas suivi le rythme voulu.
- *Que le directeur municipal renforce les pouvoirs réels de l'EGTIM, notamment en augmentant la portée des évaluations pour qu'elles englobent à l'échelle de la Ville les risques et les stratégies d'atténuation recommandées ou proposées.* La

Suivi de la vérification de 2015
de la gestion des risques liés aux technologies de l'information

Ville a mis sur pied l'Équipe de gestion des risques liés à la sécurité technologique, qui se veut un organisme de surveillance pour maîtriser les risques et prendre les décisions. Nous avons noté que les politiques et les processus actuels de gestion des risques de TI de la Ville manquent d'uniformité en ce qui concerne les approbations à délivrer pour les exemptions et les exceptions au titre des procédures normalisées qui influent la gouvernance et la surveillance des risques de TI.

- *Que le directeur municipal précise et étende les rôles et les responsabilités du directeur et chef de l'information, STI, notamment afin qu'il puisse tenir compte des meilleures pratiques décrites dans le référentiel Risk IT d'ISACA et afin que les signalements concernant les TI de tous les services et organismes municipaux lui soient adressés.* La Ville a mis à jour la Politique sur la sécurité de l'information et a préparé un cadre de gestion des risques liés à la technologie de l'information, qui décrit les rôles et les responsabilités des postes clés en ce qui a trait à ses risques de TI. Nous avons noté que ces pratiques s'harmonisent avec le référentiel Risk IT de l'ISACA et obligent à mener le processus annuel de validation des risques qu'on met actuellement au point et qui constituera un élément essentiel du suivi et de la gestion des risques de TI.
- *Que le directeur et chef de l'information, STI, élabore un cadre de gestion des risques liés aux TI solide qui :*
 - *s'harmonise avec le cadre de GAR.* Nous avons noté que le cadre de GRTI a été élaboré et que l'harmonisation est en place.
 - *inclue des sections consacrées à la gouvernance dans le cadre de gestion des risques liés aux TI (voir recommandation 1).* Comme nous l'avons mentionné ci-dessus, nous avons noté que les politiques et les processus actuels de gestion des risques de la Ville manquent d'uniformité en ce qui concerne les approbations à délivrer pour les exemptions ou les exceptions au titre des procédures normalisées, ce qui influe sur la gouvernance et la surveillance des risques de TI.
 - *définit les rôles, les responsabilités et les pouvoirs de tous les employés municipaux responsables de la gestion des risques liés aux TI.* Comme nous l'avons mentionné ci-dessus, nous avons noté que les politiques et les processus actuels de gestion des risques de TI de la Ville manquent d'uniformité en ce qui concerne les approbations à délivrer pour les exemptions

Suivi de la vérification de 2015
de la gestion des risques liés aux technologies de l'information

- ou les exceptions au titre des procédures normalisées (ce qui influe sur la gouvernance et la surveillance des risques de TI).
- *comprenne un inventaire détaillé de l'écosystème des TI et un registre des risques.* On n'a pas établi le périmètre du parc de TI qui permettrait de recenser les risques potentiels de TI. Il existe un registre des risques, et l'on a mené récemment un examen trimestriel.
 - *propose un mécanisme de vérification efficace géré par des professionnels des TI qualifiés et formés.* Au moment de l'évaluation, nous avons observé deux mécanismes qui s'appliquent dans la fonction d'analyse des risques de TI : processus régissant les exemptions et les exceptions, qui manquent d'uniformité, d'après ce que nous avons observé, en ce qui concerne les approbations à délivrer dans le cadre des pratiques de la Ville, et le processus annuel de validation des risques, qui était en voie d'élaboration; nous avons noté que les personnes-ressources affectées à ce processus devaient être mieux secondées pour ce qui est de la formation, de l'expérience et du temps à consacrer à l'établissement de ce processus.
 - *garantit que les stratégies d'atténuation des risques qui excèdent le seuil de tolérance soient communiquées à la haute direction de manière exhaustive et efficace.* Il existe un registre des risques opérationnels, qui sert à faire connaître les risques dans un tableau de bord. Le personnel des Services de soutien aux activités joue le rôle de personne-ressource à contacter dans les directions générales pour toutes les activités de gestion des risques, et nous avons noté que ce personnel n'a pas les connaissances technologiques ni la formation rigoureuse dans la gestion des risques pour pouvoir dépister les risques potentiels de TI et participer à l'évaluation des risques de TI.
 - *Que le directeur et chef de l'information, STI élabore des politiques et des procédures complémentaires au cadre de gestion des risques liés aux TI qui :*
 - *comprennent les processus nécessaires à la mise en œuvre du cadre de gestion des risques liés aux TI et d'un mécanisme de vérification solide.* Comme nous l'avons mentionné ci-dessus, nous avons noté que le processus annuel de validation des risques était en voie d'élaboration au moment de l'évaluation, ce qui constitue un élément essentiel du cadre de GRTI, et nous avons noté que d'après nos observations, le processus régissant les

Suivi de la vérification de 2015
de la gestion des risques liés aux technologies de l'information

exemptions et les exceptions manquaient d'uniformité pour ce qui est des approbations à délivrer.

- *décrivent les compétences et la formation que doivent détenir les employés responsables d'élaborer les documents de gestion des risques liés aux TI spécifiques aux différents services.* Nous n'avons pas relevé de pièces justificatives confirmant que les ensembles de compétences et les spécifications de la formation pour les volets généraux des documents de la GRTI étaient précisés.
- *intègrent le rôle élargi du directeur et chef de l'information, STI.* Nous avons noté que des progrès considérables ont été accomplis pour mieux définir le rôle du chef de l'information depuis la mission de vérification précédente. Or, le rôle du chef de l'information dans les politiques et les processus de gestion des risques de TI à l'heure actuelle manque de cohésion en ce qui concerne les approbations à délivrer pour les exemptions ou les exceptions au titre des procédures normalisées.
- *Que tous les services, avec le soutien du STI :*
 - *s'assurent que le personnel responsable d'élaborer les documents de gestion des risques liés aux TI dispose des compétences et des outils adéquats.* Comme nous l'avons mentionné ci-dessus, le personnel des Services de soutien aux activités joue le rôle de personne-ressource dans les directions générales pour toutes les activités de gestion des risques, et nous avons noté qu'il n'a pas les connaissances technologiques ni la formation rigoureuse dans la gestion des risques de TI pour pouvoir répertorier les risques potentiels de TI et participer à l'analyse voulue des technologies complexes afin de pouvoir s'acquitter de ses responsabilités dans l'évaluation des risques de TI. En outre, nous avons noté que l'approche adoptée pour mener un processus d'examen rapide afin de capter les risques de TI existants en faisant appel à l'information existante de l'ÉMR ne permet pas de dépister correctement tous les risques qui doivent être évalués dans l'administration municipale, et il se pourrait qu'on doive faire appel à d'autres personnes-ressources au sein des STI pour procéder à l'évaluation des risques et exercer les activités de planification et de surveillance pour maîtriser les risques correspondants.

Suivi de la vérification de 2015
de la gestion des risques liés aux technologies de l'information

- *élaborent leurs propres processus afin de garantir que tous leurs éléments de TI soient inclus dans les documents de gestion des risques liés aux TI.* Nous avons noté que le processus annuel de validation des risques était en voie d'élaboration au moment de l'évaluation; il s'agit d'un élément essentiel du cadre de GRTI.
- *mettent en place des mécanismes d'évaluation et de vérification qui garantissent que les documents de gestion des risques liés aux TI sont suffisamment détaillés, de manière à faciliter la compréhension des risques liés aux TI, des répercussions, de la gestion et des stratégies d'atténuation.*
Comme nous l'avons mentionné ci-dessus, nous avons noté que le processus annuel de gestion des risques était en voie d'élaboration au moment de l'évaluation; il s'agit d'un élément essentiel du cadre de GRTI; nous avons également noté que le processus régissant les exemptions et les exceptions manquait d'uniformité pour ce qui est des approbations à délivrer.

Voici les recommandations que nous n'avons pas pu évaluer :

- *Que le directeur et chef de l'information, STI et les gestionnaires de tous les services continuent d'améliorer la détection et l'évaluation des risques liés aux TI, ainsi que les stratégies d'atténuation connexes, en se reportant au cadre de gestion des risques liés aux TI (voir recommandations 1 et 2).* Le cadre de GRTI a été établi en 2018; ce cadre doit être revu et mis à jour chaque année. Puisque l'échéance prévue pour la révision annuelle n'était pas encore passée au moment de l'évaluation et que la révision annuelle n'avait pas encore été faite, nous n'avons pas pu évaluer l'application de cette recommandation.

Conclusion

La direction a accompli peu de progrès dans la mise en œuvre des recommandations découlant de la Vérification de la gestion des risques de TI. En particulier, selon notre évaluation, sept des huit recommandations ont été appliquées en partie seulement, et la huitième n'a pas pu être évaluée dans le cadre de ce suivi.

Bien que selon les réponses de la direction, dans bien des cas, les recommandations ont été appliquées d'après la mise en œuvre du Cadre de gestion des risques de TI de la Ville et différents processus comme le processus de l'évaluation des risques, le processus de l'exemption des risques et le processus annuel de validation des risques,

Suivi de la vérification de 2015 de la gestion des risques liés aux technologies de l'information

entre autres, on n'a pas fourni aux vérificateurs des pièces justificatives suffisantes pour confirmer que ces processus ont été mis en œuvre avec succès ou correctement.

D'après les processus consignés par écrit par la Ville et les discussions tenues avec le personnel des STI, un volet essentiel de l'analyse de la posture de risque de la Ville prévoit un processus annuel de validation des risques. Ce processus n'a pas encore été parfaitement élaboré ni consigné par écrit; toutefois, on y fait massivement appel pour dépister les risques dans l'administration municipale. Compte tenu de l'envergure et de la complexité des initiatives de gestion des risques, la Ville devrait se demander si elle devrait continuer de consacrer des ressources aux fonctions de gestion des risques de TI.

En outre, les représentants des Services de soutien aux activités (SSA) de la Ville sont chargés de dépister et de communiquer les risques potentiels de TI, en plus de participer aux évaluations portant sur les risques; dans bien des cas, le personnel les appelle les « praticiens des risques ». Nous avons noté que ces personnes-ressources manquaient aussi de connaissances technologiques et de formation rigoureuse dans la gestion des risques de TI pour pouvoir dépister les risques potentiels de TI et participer à l'évaluation des risques de TI.

Bien que le processus d'évaluation des menaces et des risques (ÉMR) en vigueur soit conçu pour permettre de dépister les risques de TI d'après les nouveaux projets, les nouvelles initiatives ou l'évolution des technologies, ce processus ne permet pas de dépister les risques de TI dans les technologies existantes que la Ville utilise et qui n'ont pas fait l'objet de nouveaux projets, de nouvelles initiatives ou de modifications.

Pour le dépistage des risques de TI dans les technologies existantes dans l'administration municipale, les STI ont mené un projet pilote pour deux des 53 secteurs d'activité de la Ville afin de connaître l'effort à consacrer à la captation des risques de TI. Dans la foulée de ce projet pilote, la direction a décidé qu'il ne valait sans doute pas la peine de consacrer tant d'efforts en obligeant les secteurs d'activité à capter les risques de TI dans le cadre de séances d'information sur les risques. On a plutôt fait appel à une approche qui prévoit un processus d'examen rapide d'après l'information existante de l'ÉMR afin de produire les profils de gestion des risques des secteurs d'activité, qui sont ensuite soumis à des validations annuelles des risques technologiques. (Ce processus de validation était toujours en voie d'élaboration au moment de cette mission de vérification de suivi.) On n'a pas remis, à l'équipe de vérificateurs, la liste des systèmes qui avaient fait l'objet d'une ÉMR.

Suivi de la vérification de 2015 de la gestion des risques liés aux technologies de l'information

Les vérificateurs notent que cette approche, de concert avec un univers de risques de TI incomplet, ne permet sans doute pas de dépister tous les risques qui doivent être évalués dans l'administration municipale et qu'il pourrait se révéler nécessaire de faire appel à d'autres personnes-ressources au sein des STI pour procéder à l'évaluation des risques et exercer les activités connexes de planification et de surveillance pour la maîtrise des risques (par exemple, pour opérationnaliser le processus annuel de validation des risques). Compte tenu de l'importance organisationnelle et de la complexité de la Ville, et puisque tout le programme de gestion des risques n'a pas encore été entièrement opérationnalisé, il est improbable qu'il soit possible d'avoir une vue d'ensemble complète du périmètre des risques de TI de la Ville compte tenu des ressources disponibles à l'heure actuelle, ce qui restreint la capacité de la Ville à dépister les risques de TI et à leur attribuer des priorités pour les maîtriser dans les plus brefs délais et pour les harmoniser stratégiquement afin de rehausser la valeur organisationnelle.

Nous avons aussi noté que les politiques et les processus actuels de gestion des risques de TI de la Ville manquent d'uniformité en ce qui concerne les rôles, les responsabilités et les pouvoirs liés aux approbations à délivrer pour les exemptions et les exceptions au titre des procédures normalisées. Ce manque d'uniformité dans les pratiques a aussi une incidence sur la gouvernance et sur la surveillance des risques de TI, puisqu'elle se répercute sur six des huit recommandations déjà exprimées. Le *Cadre de gestion des risques de TI* (daté du 18 janvier 2018), la *Politique sur la sécurité de l'information* (datée du 16 juillet 2018) et le *Processus d'exemption des risques de sécurité techniques* (daté du 7 septembre 2018) comportent des renseignements contradictoires pour les approbations et les autorisations se rapportant à l'approbation des exemptions et des exceptions au titre des procédures normalisées. Selon le document visé, l'équipe de la haute direction, l'équipe de la GRST ou le chef de l'information et le chef de la direction générale doivent approuver les exemptions et les exceptions au titre des risques [élevés]. Dans la pratique, nous avons observé que les exemptions examinées (par exemple, une exemption liée au module du serveur des élections et une exception liée à l'archivage des adresses de courriel et des numéros de téléphone personnels aux États-Unis dans le cadre d'un déploiement infonuagique) n'ont pas été approuvées par l'équipe de la haute direction ou les responsables de la GRST et qu'ils ont été approuvées par le chef de l'information ou par le gestionnaire de la Sécurité des TI. C'est pourquoi nous ne pouvons pas, dans notre évaluation, savoir si ces exceptions ou exemptions ont respecté la politique ou le processus voulu; toutefois,

Suivi de la vérification de 2015 de la gestion des risques liés aux technologies de l'information

le processus de GRTI et le processus régissant les exemptions au titre des risques pour la sécurité technique laissent tous deux entendre qu'il aurait fallu demander aussi l'approbation de l'équipe de la haute direction ou des responsables de la GRST, ce qui nuit à l'efficacité de la surveillance de ces organismes de gouvernance. En outre, nous avons noté que l'exemption qui autorisait l'archivage, aux États-Unis, des renseignements permettant d'identifier des personnes a été soumise et approuvée par le chef de l'information de la Ville; il n'existe pas de politique ni de processus indiquant qu'il s'agit d'une pratique admissible. Nous invitons la Ville à se pencher sur les enjeux potentiels liés à cette pratique.

Remerciements

Nous tenons à remercier la direction pour la collaboration et l'assistance accordées à l'équipe de vérification.