Bureau du vérificateur général

Vérification de la gestion des risques liés aux technologies de l'information

Résumé

Déposé devant le Comité de la vérification – Le 26 novembre 2015

Table des matières

Résumé

Introduction

Le Plan de vérification de 2014 de la Ville d'Ottawa, approuvé par le Conseil en mars 2014, prévoit des vérifications des technologies de l'information (TI) et des investissements en cette matière. La présente vérification de la gestion des risques liés aux TI et la vérification de la gestion des incidents de sécurité des TI et des interventions connexes ont été effectuées conformément au Plan de vérification de 2014.

Contexte

Les solutions et innovations fondées sur les TI contribuent à l'atteinte de divers objectifs stratégiques et opérationnels dans tous les services de la Ville. Des solutions novatrices sont sans cesse créées, et on s'attend à ce que l'importance des technologies continue d'augmenter très rapidement. Toutefois, mçeme 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 organisation 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.

L'approche municipale de gestion des risques liés aux TI

Le cadre de gestion améliorée des risques

En 2010, le Conseil a approuvé un cadre conceptuel de gestion améliorée des risques (GAR) et la Politique de la Ville d'Ottawa sur la gestion améliorée des risques. En 2011, le cadre avait été mis en œuvre dans tous les services municipaux. Il définit le processus municipal de gestion des risques et les rôles et responsabilités qui y sont associés, de même que les outils et les ressources qui sont à la disposition des gestionnaires de service et des autres personnes habilitées par le cadre et la politique. Depuis 2011, les services municipaux effectuent annuellement des analyses des risques, ce qui a mené à la constitution du profil de risque municipal.

Risques liés aux TI

L'expression « risques liés aux TI » désigne tous les risques posés par l'utilisation, la possession, la participation, les effets et l'adoption des TI dans une organisation. Il s'agit de tous les événements liés aux TI qui pourraient entraver la réalisation des objectifs de l'organisation. Comme pour la plupart des risques, l'ampleur des dommages et la fréquence à laquelle les risques se concrétiseront sont par définition imprévisibles. Parmi les risques liés aux TI, on compte la perte ou la corruption de données et l'incapacité de l'organisation à remplir les fonctions qui en dépendent.

Cadre de 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.

Le STI joue 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, le STI est chargé d'élaborer des politiques et des lignes directrices encadrant la gestion des risques liés aux TI.

Le STI est officiellement responsable 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.

Objectifs et portée

Objectif n^{o} 1

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

Objectif n^{o} 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.

Objectif no 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.

La présente vérification avait pour objet les activités de gestion des risques liés aux TI de tous les services municipaux. Elle a nécessité l'examen de la conception et de l'efficacité des mesures (politiques, pratiques et procédures) ainsi que des rôles et des responsabilités du personnel du STI et des autres services qui utilisent des TI, notamment ceux qui ont recours à une équipe de TI autonome.

Résumé des principales constatations

Gouvernance, leadership des cadres et soutien

La Ville s'appuie sur différents comités pour assurer la gestion des risques liés aux TI. À la suite de la présentation de la vérification de la gouvernance des TI en mars 2015, la structure de reddition de comptes a été renforcée, en dépit de quelques lacunes soulignées dans la présente vérification.

La Ville a dû composer avec un taux de roulement passablement élevé au poste de directeur et chef de l'information, Service de technologie de l'information, au cours des dernières années, sans compter de longues périodes d'intérim. Un nouveau directeur et chef de l'information, STI, a été embauché au printemps 2015. Le personnel des STI interrogé dans le cadre de la vérification s'est montré optimiste et enthousiaste par rapport au leadership, à la direction stratégique et au soutien du nouveau titulaire.

Malgré ces progrès, la Ville ne dispose toujours pas d'un cadre de gestion des risques liés aux TI comportant une section consacrée à la gouvernance, qui préciserait de manière claire et cohérente les responsabilités des cadres et les gestionnaires municipaux. Plus particulièrement, l'efficacité de la gouvernance relativement au cadre de gestion des risques liés aux TI est diminuée par de nombreux facteurs, notamment :

a) l'absence d'un cadre de gestion des risques liés aux TI comportant une section consacrée à la gouvernance;
b) la priorisation, la sélection et le financement des initiatives de TI;
c) les pouvoirs de l'Équipe de gestion de la technologie de l'information municipale (EGTIM);
d) les pouvoirs du directeur et chef de l'information, STI.

Ces points sont traités en détail ci-après.

Cadre de gestion des risques liés aux TI comportant une section consacrée à la gouvernance

Bien que le cadre de GAR en contienne quelques-uns des éléments, la Ville n'a pas de cadre autonome de gestion des risques liés aux TI comportant une section consacrée à la gouvernance, indispensable à la gestion adéquate des risques. Une gouvernance efficace s'appuyant sur un cadre de gestion des risques liés aux TI contribuerait à baliser clairement la tolérance au risque de la Ville et à superviser la mise en œuvre des mesures qui s'y rattachent. Sans une orientation claire et une supervision efficace de ces éléments, il est impossible d'élaborer un cadre de gestion des risques liés aux TI (veuillez consulter la section intitulée « Conception et orientation du cadre de gestion des risques liés aux TI » pour une discussion plus approfondie à ce sujet).

Priorisation et financement des projets de TI

Les projets de TI sont présentés aux fins d'examen par les services, qui doivent définir les sources de financement de chaque projet et sont encouragés à ne soumettre que les projets dont le financement est assuré. Bien qu'il arrive que des projets non financés soient approuvés et qualifiés d'investissements prioritaires, cette approche signifie que les projets approuvés ne s'accordent pas toujours avec les priorités de la Ville.

La marge de manœuvre est limitée pour ajuster les budgets d'infrastructure du STI et des autres services afin de financer les projets de TI hautement prioritaires, puisque la grande partie des budgets alloués aux TI sont gérés par les services eux-mêmes et non par le STI. Certains services (Service de transport en commun, Service de la circulation et Services d'eau) ont des budgets considérables alloués aux TI et des équipes de TI autonomes. En général, ces budgets ont été établis dans le passé en réponse à une situation particulière avant d'être intégrés au budget de base. Cette conjoncture favorise l'investissement de sommes consacrées à la gestion des risques liés aux TI dans certains services alors que d'autres lacunes en matière de TI et les risques qui y sont liés dans d'autres secteurs ne sont pas réglés.

Qui plus est, il existe plusieurs mécanismes de financement, certains avec leurs contraintes particulières (p. ex. le financement issu des redevances supplémentaires pour l'eau et les égouts ne peut servir qu'à certaines activités précises relatives à l'eau et aux égouts).

Par conséquent, il est fort probable que des risques majeurs liés aux TI ne soient pas pris en compte suffisamment tôt si les gestionnaires n'ont pas accès au financement requis. C'est notamment le cas de l'infrastructure de TI désuète du STI, des initiatives présentes et passées des services (p. ex. Services d'eau, Service de la circulation et Service de transport en commun) et des systèmes de gestion de l'information (GI) et de TI de certains autres services.

Pouvoirs de l'Équipe de gestion de la TI municipale (EGTIM)

Le processus d'approbation de l'EGTIM est adéquat en principe, mais il est entravé par les pratiques énumérées ci-dessus, qui font que les projets soumis à l'approbation de l'EGTIM dans le cadre du plan municipal annuel en matière de TI sont généralement ceux qui sont déjà financés, soit par les services concernés, soit par des sources externes comme le gouvernement de l'Ontario, ou encore au moyen de sommes réservées à cette fin. Ainsi, le financement des projets, et non un système municipal de priorisation en fonction des risques, est un facteur déterminant dans le choix par l'EGTIM des projets qui feront partie du plan municipal annuel en matière de TI.

Cette approche décentralisée du financement des projets de TI et l'absence d'un système municipal de priorisation en fonction des risques diminuent l'efficacité de l'EGTIM à remplir son mandat, qui consiste à assurer la planification, la supervision et l'orientation stratégique requises pour :

- produire un plan municipal annuel en matière de TI qui s'harmonise avec les plans stratégiques globaux approuvés par le Conseil et ses comités;
- tenir compte des besoins de la Ville et des différents services;
- appuyer le STI dans la réalisation de son mandat d'offrir des solutions technologiques novatrices et rentables pour maximiser la valeur opérationnelle;
- baser ses décisions sur le Plan stratégique global.

Le mandat de l'EGTIM exige par ailleurs qu'elle établisse les orientations municipales en matière de technologie, considérant que le Comité exécutif lui en a donné le pouvoir. Bien que ce ne soit pas mentionné explicitement dans son mandat, l'EGTIM a la responsabilité implicite de recommander un plan municipal en matière de TI qui reflète les priorités municipales fondées sur les risques liés aux TI. La capacité de l'EGTIM à s'acquitter de cette responsabilité 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 (voir plus bas). De ce fait, les dépenses et les investissements liés aux TI ne s'accordent pas toujours avec les priorités municipales et objectifs de gestion des risques.

Pouvoirs du directeur et chef de l'information, STI

Selon la description du poste de directeur et chef de l'information, STI, en plus de diriger le STI, le titulaire doit exercer un leadership stratégique à l'échelle globale en ce qui a trait à la planification et à la mise en œuvre d'un large éventail d'initiatives municipales de GI et de TI s'inscrivant dans les objectifs municipaux en matière de prestation des services.

Le directeur est appelé à jouer un rôle majeur de leadership dans l'organisation, la gestion et le renforcement d'une infrastructure complète de TI et de GI destinée à soutenir et à transformer l'administration et la prestation de services de la Ville, et à appuyer son mandat. Il doit également superviser la mise en œuvre des stratégies des différents services, assurer la planification financière à long terme relativement à la GI et aux TI et servir de conseiller principal sur ces questions auprès du Conseil, des comités du Conseil et des conseillers afin de leur fournir des orientations stratégiques, des avis et des renseignements techniques.

Néanmoins, la capacité du directeur à gérer et à influencer 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) est limitée puisqu'ils ne sont pas techniquement soumis à son autorité et que la hiérarchie n'est pas toujours clairement établie. En outre, l'équipe de vérification n'a pu trouver de description officielle (ni dans la description de poste, ni ailleurs) des pouvoirs et des responsabilités du directeur en ce qui a trait aux risques liés aux TI à l'échelle municipale.

Le manque de précision au sujet des rôles et des responsabilités du directeur entrave sa capacité à :

- favoriser une culture d'entreprise qui favorise l'atteinte des objectifs du cadre de gestion des risques liés aux TI, notamment en incitant la haute direction à apporter des changements, à instaurer des pratiques de gestion du changement lié aux TI dans les différents services et à gérer les dépenses municipales en matière de GI et de TI;
- aligner le financement municipal des TI aux initiatives stratégiques prioritaires globales;
- s'attaquer aux risques prioritaires en matière de TI à l'échelle de la Ville, suffisamment tôt et de façon stratégique;
- veiller au respect des politiques et des procédures, et exiger que lui soient rapportées toutes les activités rattachées au cadre de gestion des risques liés aux TI.

La structure de reddition de comptes rattachée au poste de directeur et chef de l'information, STI, n'est pas conforme aux pratiques exemplaires. Le référentiel Risk IT recommande que le titulaire du poste soit responsable de tous les processus municipaux d'évaluation et de gestion des risques, ainsi que d'intervention en la matière, et que tous les gestionnaires de TI subordonnés relèvent de lui.

Ces changements feraient en sorte que le directeur et chef de l'information, STI, ait autorité sur tous les employés rattachés aux TI, ce qui lui permettrait de renseigner et de conseiller le directeur municipal, à qui reviendrait la responsabilité de gérer les

risques liés aux TI, y compris le financement des stratégies et possibilibiltés d'atténuation. Le directeur et chef de l'information, STI, pourrait également influer sur les décisions afin de garantir que les priorités municipales (p. ex. assurer l'intégrité et la sécurité des infrastructures existantes) reçoivent l'attention et le financement nécessaires.

Cela dit, au bout du compte, pour pouvoir vraiment gérer les risques liés aux TI et saisir les occasions qui permettront de faire d'Ottawa une « ville intelligente » par excellence, le directeur et chef de l'information, STI doit se voir accorder les pouvoirs, les ressources et les moyens pour :

- gérer les coûts liés aux TI et l'incidence des dépenses en TI sur l'organisation;
- s'assurer du bon fonctionnement des mesures de sécurité liées aux TI;
- agir à titre de « courtier » de l'information pour orienter les décisions opérationnelles;
- proposer des idées et des solutions afin d'améliorer les processus municipaux en étant un partenaire d'affaires actif;
- préparer la Ville aux changements;
- améliorer les modèles opérationnels grâce à des idées novatrices et à l'utilisation de technologies appropriées.

Conception et orientation du cadre de gestion des risques liés aux TI

La Ville doit élaborer un cadre complet de gestion des risques liés aux TI. Alors que sont menées de nombreuses activités afférentes à la gestion des risques liés aux TI (p. ex. au niveau des projets et des systèmes), comme il est indiqué dans l'Objectif 1, la Ville n'a toujours 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.

Les processus de GAR sont continuellement perfectionnés, notamment par l'élaboration récente d'une classification détaillée des risques liés aux TI. Plus précisément, depuis 2015, les risques liés aux technologies, qui étaient auparavant divisés en dix sous-catégories difficiles à différencier, se classent dorénavant en six sous-catégories faciles à distinguer : 1) entretien et cycle de vie; 2) non-disponibilité des ressources; 3) perturbations et interruptions du service; 4) médias sociaux; 5) mise à niveau des logiciels et du matériel informatique; 6) défaillance du système. Cette nouvelle classification des risques est plus claire et correspond beaucoup mieux à la nature des cas rencontrés.

Cependant, bien que la Ville ait commencé récemment à recenser les risques liés aux TI et à les intégrer au cadre de GAR, 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 nombreux facteurs, notamment :

- 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.

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.

Ces points sont traités en détail ci-après.

Cadre de gestion des risques liés aux TI – Rôles et responsabilités

Les responsabilités des employés qui contribuent à l'élaboration de documents de gestion des risques liés aux TI (p. ex. des registres de risques) ne sont pas décrites en détail, mis à part la création du profil de risque municipal dans le cadre du processus de GAR. On s'attendait à ce que les rôles et les responsabilités du personnel chargé des processus de gestion des risques liés aux TI soient énoncés clairement et de façon systématique, et comportent un modèle de type RACI (Responsable – Agent comptable – Consulté – Informé) intégré dans un cadre de gestion des risques liés aux TI comprenant les politiques et procédures requises. Comme il a été mentionné plus haut, les pratiques avant-gardistes élaborées par ISACA ont servi de critères pour mesurer l'efficacité de la gestion des risques liés aux TI à la Ville. L'évaluation portait plus particulièrement sur les aspects « **Responsable** » (le personnel responsable de l'exécution réussie des activités) et « **Agent comptable** » (les gestionnaires qui

disposent des ressources et des pouvoirs nécessaires pour approuver la mise en œuvre d'une activité ou son résultat) des processus du référentiel Risk IT. Les lacunes du cadre de gestion des risques liés aux TI ont une incidence sur la capacité de la Ville à :

- intégrer la gestion des risques liés aux TI à la GAR, afin de prendre des décisions fondées sur le rapport risque-rendement;
- mettre en place un mécanisme efficace pour vérifier l'exhaustivité et l'exactitude de la détection et de l'évaluation des risques;
- prendre des décisions éclairées en fonction de la portée des risques et de sa tolérance au risque;
- comprendre comment répondre aux risques.

Politiques et procédures

Les politiques et les procédures municipales actuelles, y compris la Politique de gestion des risques liés aux informations, sont conformes au cadre de GAR. Toutefois, les services, y compris ceux qui ont recours à une équipe autonome, sont peu supervisés par rapport à leurs pouvoirs et à leurs responsabilités alors qu'ils mènent des activités qui pourraient avoir des répercussions sur le profil de risque de la Ville. Les politiques existantes mettent surtout l'accent sur les menaces à la sécurité et les violations de confidentialité; c'est entre autres le cas de la Politique sur l'utilisation responsable des ordinateurs et de la politique sur les appareils numériques. Par contre, il manque une politique pour encadrer les activités à risque comme l'utilisation de l'infonuagique ou de systèmes et d'appareils externes.

Qui plus est, la plupart des services :

- n'ont pas élaboré de politiques ni de procédures qui reflètent les risques liés aux TI propres à leurs objectifs et à leur contexte;
- dépendent des processus annuels de GAR, des interventions du STI et d'activités à portée restreinte (p. ex. les évaluations de la vulnérabilité) pour gérer les risques liés aux TI.

Formation et compétences

La Ville offre des formations sur les systèmes de TI et les logiciels de GI. Ces formations portent principalement sur la sécurité; il y a donc un manque à combler en ce qui a trait à l'utilisation efficace des TI.

Dans certains services, en vertu du cadre de GAR, des employés n'ayant reçu que peu de formation technique (voire aucune) sont chargés de la détection et de l'atténuation des risques. Par conséquent, il y a des lacunes en matière de détection, d'évaluation et d'atténuation d'importants risques liés aux TI (sécurité, confidentialité, intégrité,

disponibilité, réputation, opérations, conformité aux normes et aux lois, stratégies, continuité des opérations, etc.).

Plan municipal de technologie opérationnelle et Plan stratégique du STI

Le Plan stratégique du STI de 2011-2014 décrit comment le STI contribuera à la réalisation de la vision pour le mandat précédent du Conseil en fournissant des renseignements sur les objectifs stratégiques et les initiatives connexes du STI, et sur la manière dont elles s'harmonisent avec les priorités stratégiques municipales. Bien que le plan comprenne quelques détails sur les initiatives stratégiques du STI (p. ex. droits de propriété, descriptions et évaluation du rendement), sa portée est limitée puisqu'il présente une stratégie de TI du point de vue du Service et non de la Ville en général.

Le Plan de technologie opérationnelle présente quant à lui une vision à l'échelle de la Ville. Il propose un résumé des activités prévues, dont celles rattachées à ServiceOttawa, aux nouveaux projets, aux initiatives municipales en cours et au soutien opérationnel. L'équipe de vérification a revu la documentation (chartes de projets, scénarios, évaluations des risques, stratégies de gestion du changement, plans de mise en œuvre, etc.) liée à trois (3) projets de TI. Tous les projets ne démontrent pas qu'ils s'accordent avec les priorités municipales, mais le plus récent comportait des références aux priorités du Conseil et des renseignements sur la manière dont le projet allait contribuer à ces priorités. Il est important qu'à l'avenir les liens avec les priorités du Conseil soient toujours clairement démontrés.

Écosystème des risques liés aux TI

Le processus de détection des risques liés aux TI est entravé avant tout par l'absence d'un inventaire complet de l'« écosystème » de TI de la Ville (logiciels, responsables opérationnels, réseaux, interdépendances, etc.). De plus, il n'y a pas de registre complet des risques (risques, répercussions, stratégies d'atténuation, état, etc.) élaboré par des professionnels qualifiés et formés des TI.

Les risques sont accrus par la présence de nombreuses équipes de TI complètement ou partiellement indépendantes du STI au sein des différents services (p. ex. Services d'eau, Direction de la gestion des eaux usées, Service de transport en commun et Direction de la circulation routière). En plus de recourir à des équipes autonomes, ces services utilisent des logiciels qui ne sont pas contrôlés par la Ville (p. ex. des logiciels prescrits par la loi provinciale utilisés par Santé publique Ottawa). De même, de nombreux services ont acquis des logiciels externes ou utilisent des solutions d'infonuagique sans la supervision du STI. Ces logiciels présentent des risques liés aux TI dans la mesure où on les utilise en ayant recours aux ordinateurs et aux réseaux municipaux, et en étant connecté à l'infrastructure de TI de la Ville. Les risques sont

élevés, particulièrement lorsque ces logiciels contiennent des renseignements personnels et confidentiels sur les résidents d'Ottawa.

En outre, plusieurs systèmes plus anciens continuent de s'appuyer sur une infrastructure de TI vétuste. En général, les ressources de fonctionnement et de maintenance de ces systèmes et des infrastructures de TI connexes sont très élevées.

Sans un inventaire complet, exhaustif et documenté du matériel et des logiciels de TI qui dépendent de l'infrastructure municipale, il est impossible d'établir un registre des risques détaillé qui recense les risques et les répercussions ainsi que les stratégies d'atténuation et les mesures correctives nécessaires.

Efficacité de l'approche de gestion des risques liés aux TI

Les questions de gouvernance et de conception mentionnées précédemment ont des répercussions considérables sur l'efficacité de la gestion des risques liés aux TI à la Ville. Bien que les processus et les politiques de la GAR et du profil de risque municipal soient respectés et que les risques liés aux TI soient régulièrement détectés, évalués et atténués dans la cadre de la GAR et d'autres activités, les problèmes suivants persistent en ce qui concerne la qualité et l'exhaustivité de la gestion de risques :

- 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'examens 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.

De même, l'analyse de la catégorie « TI » du profil de risque municipal montre que ce dernier ne contient pratiquement aucun renseignement sur les risques liés aux TI, comme ceux soulevés dans le rapport sur la gestion des incidents touchant la sécurité, notamment en ce qui concerne l'impartition, les logiciels externes, l'infonuagique, la supervision des fournisseurs de TI, la reprise après sinistre, la continuité opérationnelle, la gestion des licences de logiciels, les services informatiques pour les utilisateurs finaux, la capacité des infrastructures de TI et les coûts de GI.

Comme nous l'avons remarqué plus haut, sans un inventaire complet et exhaustif de l'écosystème des TI, il ne peut y avoir de vision d'ensemble des risques liés aux TI et la Ville ne peut prendre des décisions éclairées à ce sujet. En effet, la Ville ne peut pas prendre des décisions qui tiennent compte des possibilités et des conséquences qu'entraîne l'utilisation des TI. De plus, il est impossible pour les employés, ceux du STI en particulier, de comprendre tous les risques potentiels liés aux TI, puisqu'ils ne peuvent détecter les risques dont ils n'ont pas connaissance ni anticiper les mesures correctives à mettre en œuvre.

Recommandations et réponses de la direction

Recommandation 1

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;**
- **définisse clairement les rôles, les responsabilités et les pouvoirs des cadres supérieurs et des gestionnaires;**
- **jette les bases d'une culture organisationnelle des risques qui tient compte des lignes directrices concernant la tolérance au risque;**
- **tient compte des stratégies d'atténuation des risques qui excèdent le seuil de tolérance lors de l'élaboration du plan municipal annuel en matière de TI, et ce, en fonction de la nature du risque, peu importe qu'il y ait du financement approuvé préalablement ou pas.**

Réponse de la direction

La direction est d'accord avec cette recommandation.

Le directeur municipal travaillera avec le Service de technologie de l'information (STI) et le Service des programmes municipaux et des services opérationnels pour élaborer une section consacrée à la gouvernance dans un cadre de gestion des risques liés aux technologies de l'information (TI). Les mesures visant à appliquer cette recommandation seront mises en œuvre en parallèle avec celles visant à appliquer la recommandation 5. La mise en œuvre de cette recommandation sera terminée d'ici le quatrième trimestre de 2016.

Recommandation 2

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.

Réponse de la direction

La direction est d'accord avec cette recommandation.

Le directeur municipal travaillera avec le Service de technologie de l'information (STI) et le Service des programmes municipaux et des services opérationnels pour élaborer une section consacrée à la gouvernance dans un cadre de gestion des risques liés aux technologies de l'information (TI). Les mesures visant à appliquer cette recommandation seront mises en œuvre en parallèle avec celles visant à appliquer la recommandation 5. La mise en œuvre de cette recommandation sera terminée d'ici le quatrième trimestre de 2016.

Recommandation 3

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.

Réponse de la direction

La direction est d'accord avec cette recommandation.

Le directeur municipal, de concert avec le STI, fera en sorte de renforcer les pouvoirs de l'Équipe de gestion de la technologie de l'information municipale (EGTIM) dans le cadre des mesures mises en œuvre pour appliquer la recommandation 1. Des procédures seront mises en place pour permettre une surveillance du processus décisionnel d'atténuation des risques par un organisme se rapportant à la haute direction. Cette tâche sera terminée d'ici le quatrième trimestre de 2017.

Recommandation 4

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.

Réponse de la direction

La direction est d'accord avec cette recommandation.

Le directeur municipal fera en sorte de confirmer et de renforcer les rôles et les responsabilités du directeur, Service de technologie de l'information et du chef de

l'information. De plus, dans le cadre des mesures mises en œuvre pour appliquer la recommandation 1, le directeur municipal prendra en considération les pratiques exemplaires soulignées dans le référentiel Risk IT d'ISACA afin d'établir des procédures de signalement des risques liés aux TI. La mise en œuvre de cette recommandation sera terminée d'ici le quatrième trimestre de 2016.

Recommandation 5

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;**
- **inclue des sections consacrées à la gouvernance dans le cadre de gestion des risques liés aux TI (voir recommandation 1);**
- **définisse les rôles, les responsabilités et les pouvoirs de tous les employés municipaux responsables de la gestion des risques liés aux TI;**
- **comprenne un inventaire détaillé de l'écosystème des TI et un registre des risques;**
- **propose un mécanisme de vérification efficace géré par des professionnels des TI qualifiés et formés;**
- **garantisse que les stratégies d'atténuation des risques qui excèdent le seuil de tolérance soient communiquées à la haute direction de manière exhaustive et efficace.**

Réponse de la direction

La direction est d'accord avec cette recommandation.

Le cadre de gestion améliorée des risques (GAR) actuel sera révisé, et le cadre de gestion des risques liés aux TI sera amélioré afin d'inclure tous les pouvoirs, les politiques et les procédures en vigueur à la Ville. Nous élaborerons des lignes directrices concernant la tolérance au risque afin que les risques inacceptables soient signalés aux autorités compétentes. L'exercice annuel d'élaboration du budget comportera une étape de définition des besoins de financement rattachés à l'atténuation des risques. La mise en œuvre de cette recommandation sera terminée d'ici le quatrième trimestre de 2017.

Recommandation 6

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;**

- **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;**
- **intègrent le rôle élargi du directeur et chef de l'information, STI.**

Réponse de la direction

La direction est d'accord avec cette recommandation.

Nous élaborerons des politiques et des procédures afin d'ajouter au cadre de gestion des risques liés aux TI un mécanisme de vérification solide. La formation et les compétences requises seront cernées et ajoutées au cadre. La mise en œuvre de cette recommandation sera terminée d'ici le quatrième trimestre de 2017.

Recommandation 7

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;**
- **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;**
- **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.**

Réponse de la direction

La direction est d'accord avec cette recommandation.

La direction de la Ville, avec le soutien du STI, intégrera la formation, la préparation de documents, le signalement des risques et les mécanismes de vérification, de suivi et de signalement au déploiement dans tous les services de la Ville du cadre de gestion des risques liés aux TI. La mise en œuvre de cette recommandation sera terminée d'ici le quatrième trimestre de 2017.

Recommandation 8

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).

Réponse de la direction

La direction est d'accord avec cette recommandation.

Le principe d'amélioration continue sera appliqué lors des différentes étapes de mise en œuvre du cadre de gestion des risques liés aux TI, afin d'améliorer constamment la détection, l'évaluation et les stratégies d'atténuation des risques liés aux TI. Un organisme de surveillance se rapportant à la haute direction, actuellement en cours de création, supervisera l'évolution du cadre de gestion des risques liés aux TI. Une fois le cadre de gestion des risques liés aux TI mis en œuvre, le STI évaluera annuellement les nouvelles stratégies d'atténuation des risques.

Économies potentielles

Nous croyons que la mise en œuvre des recommandations ci-dessus augmentera l'efficacité opérationnelle globale des façons suivantes :

- en améliorant l'orientation, les conseils et la reddition de comptes en matière de TI dans tous les services, ce qui permettra de réaliser des économies d'échelle et de rendre plus efficace la prise de décision relativement à la GI et aux TI;
- en améliorant les initiatives de détection, d'évaluation et d'atténuation des risques de façon à protéger la Ville des défaillances de système et des brèches de sécurité (y compris les cyberattaques) qui nuisent à ces activités et peuvent même avoir des répercussions sur la sécurité des personnes et la vie quotidienne des résidents. Autrement, ce type d'événement fâcheux peut coûter très cher et miner la confiance de la population envers la Ville.
- En améliorant les politiques et les procédures de façon à réduire le gaspillage et à réaliser des économies immédiates. Par exemple, les ressources et les coûts liés aux infrastructures nécessaires pour répondre aux demandes de GI sont toujours élevés, surtout si ces demandes (p. ex. logiciels, gestion des courriels) ne sont pas rigoureusement supervisées et encadrées par des politiques, des pratiques et des mesures de sensibilisation. Un suivi plus serré des risques et des coûts entraînés par les infrastructures superflues pourrait permettre de réaliser des économies immédiates.

Malgré ces économies potentielles, il est à noter que les changements requis pour renouveler les infrastructures de la Ville et améliorer la protection contre les risques liés aux TI nécessiteront des investissements considérables au cours de prochaines années.

Conclusion

Notre évaluation des documents et des stratégies de gestion des risques liés aux TI nous permet de conclure que la plupart des services municipaux présentent des lacunes à cet égard. Cela résulte principalement des problèmes de gouvernance et de

leadership observés, énoncés dans les constatations clés. Les recommandations 1 à 4 sur la gouvernance en ce qui a trait à la gestion des risques liés aux TI devront être mises en œuvre avant les recommandations 5 à 8 concernant le cadre de gestion des risques liés aux TI. Une fois les recommandations sur la gouvernance mises en place, il sera plus facile d'appliquer efficacement le reste des recommandations.

Faute de suivre les recommandations et d'élaborer un cadre de gestion des risques liés aux TI qui définit les rôles, les responsabilités, des modèles de financement et des politiques, la vulnérabilité aux risques pourrait entraîner des répercussions importantes sur les activités de la Ville. Nous recommandons fortement que la Ville élabore un plan d'action en matière de gestion en se fondant sur nos recommandations et sur les pratiques exemplaires décrites par ISACA dans COBIT et dans le référentiel Risk IT.

Remerciements

Nous souhaitons exprimer notre reconnaissance pour l'aide et la coopération de la direction à notre endroit.