Ottawa

Bureau du vérificateur général

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

Déposé devant le Comité de la vérification
Le 29 mai 2019

Table des matières

Résumé

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.

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 (EGTIM[1]) 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;
   - 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

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

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.
   - 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'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.

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

Tableau 1 : 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;
  - *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 xxxx, 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 xxxx, 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 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 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 exemptions et les exceptions manquait 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.

- *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, 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.

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, 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.

Rapport détaillé – Avancement de la mise en œuvre

Pour procéder à l'évaluation, les vérificateurs ont passé en revue les textes des politiques et des processus essentiels de la Ville, notamment le Cadre de gestion des risques liés aux TI 1.0, le processus d'exemption des risques, le processus d'évaluation des risques et des ÉMR et la Politique sur la sécurité de l'information, entre autres.

Les vérificateurs ont également tenu de nombreuses entrevues avec différents membres de l'équipe de la sécurité de l'information de la DGSTI, dont le chef de l'information de la Ville, le gestionnaire des Solutions technologiques, le gestionnaire de la Sécurité de la technologie, ainsi que différents analystes de la sécurité de la TI.

Dans le cadre de cette vérification, il a aussi fallu examiner le processus régissant les exceptions dans l'évaluation des risques. Dans le cadre de cet examen, les vérificateurs ont sélectionné la liste complète des exceptions depuis la mise en place du processus, notamment :

- Cisco Jabber – juin 2018;
- Hana de SAP – septembre 2018;
- Split Tunnel de SPO – février 2018;
- rétablissement des mots de passe dans O365 – janvier 2018;
- équipes Microsoft – mars 2018;
- économiseur d'écran EPS – septembre 2017;
- module du serveur des élections – août 2018.

Le présent rapport résume l'évaluation de la direction concernant l'état d'avancement de la mise en œuvre pour chacune des recommandations en date d'août 2018, ainsi que l'évaluation du Bureau du vérificateur général (BVG) en date de décembre 2018.

Recommandation nº 1

Tableau 2 : Avancement

Mise à jour de la direction	Évaluation du BVG
Partiellement achevée	Partiellement achevée

Recommandation de la vérification :

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;
- définit 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 initiale 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.

Mise à jour de la direction :

La Politique sur la sécurité de l’information (PSI) a été approuvée et est publiée sur Ozone. Le Cadre de gestion des risques de TI (GRTI) a été approuvé et communiqué dans l’ensemble de l’administration municipale. Ces documents décrivent dans leurs grandes lignes les rôles de la haute direction et la gouvernance des risques techniques et de sécurité technique de la Ville. Il s’agit notamment du processus formel d’exemption des risques et de l’équipe constituée pour la gouvernance de la Gestion des risques de la sécurité technique (GRST), ainsi que du processus annuel de validation des risques, dans le cadre duquel les priorités sont établies d’après les risques qui sont supérieurs aux seuils fixés.

On finalise actuellement les modalités de diffusion générale de la PSI, et l'on est en train d’élaborer le processus annuel de validation des risques; ces travaux seront achevés d’ici le quatrième trimestre de 2018.

Évaluation du BVG :

On a évalué les mesures décrites dans la mise à jour de la direction et l'on a jugé qu’elles sont partiellement achevées.

Nous avons noté que la Ville a publié le texte du Cadre de gestion des risques de TI le 18 janvier 2018. Ce nouveau cadre définit la gouvernance des risques selon quatre activités de base :

- la mobilisation des directions générales de la Ville dans la gestion des risques de TI dont elles sont responsables;
- l’examen des risques de TI à l’échelon hiérarchique voulu, selon les modalités décrites dans le Circuit de travail de la GRTI;
- l’approbation des plans d’action pour maîtriser les risques supérieurs aux seuils fixés;
- la mise à jour des politiques et des normes de la Ville pour la GRTI.

Nous avons noté que le cadre que la direction vient d’élaborer s’harmonise avec le cadre existant de la gestion des risques d’entreprise (GRE) de la Ville.

Ce cadre définit aussi les rôles de la haute direction et la gouvernance des risques techniques et de sécurité technique de la Ville. Il s’agit notamment :

- de l’équipe de la haute direction, qui est responsable de l’ensemble du programme de GRTI;

- de l'équipe de cadres de la direction générale, qui est responsable de la gestion des risques de TI et de sécurité de l'information dans sa propre direction générale;
- de l'Équipe de gestion des risques pour la sécurité des technologies, qui assure la gouvernance opérationnelle du programme de GRTI, notamment la hiérarchisation et l'approbation des exceptions;
- du chef de l'information, qui doit rendre des comptes à l'équipe de la GRST dans la gestion du programme de GRTI et qui assume la responsabilité de la GRTI de l'ensemble de l'infrastructure partagée de TI gérée par les STI;
- de la Direction de la sécurité des technologies (DST), qui est fonctionnellement responsable de nombreux volets du programme de GRTI;
- des Services de soutien aux activités (SSA), qui sont le point de contact, dans les directions générales, pour toutes les activités de gestion des risques.

En outre, nous avons noté que l'Équipe de la gestion des risques de la sécurité des technologies (GRST) est constituée :

- du directeur général de la Direction générale des services organisationnels (DGSO);
- du greffier municipal et avocat général;
- du chef de l'information.

Il est important de noter que bien que les membres de l'équipe de la GRST soient conscients des risques potentiels de leur direction générale, il se peut qu'ils n'aient pas les compétences ni l'expérience de la technologie de l'information pour comprendre parfaitement les risques de la Ville. À ce titre, c'est au chef de l'information qu'il appartient de s'assurer que l'équipe de la GRST comprend parfaitement les risques des technologies et de faire appel aux experts de la question dans les cas nécessaires.

L'Équipe de la GRST est responsable :

- de la gestion permanente des programmes d'après le registre des risques de TI, le tableau de bord et l'évaluation des risques de TI;
- de se pencher sur les questions portées à son attention par le chef de l'information et sur les changements ou les approbations dans l'ensemble du programme;
- de saisir l'équipe de la haute direction (ÉHD) des risques à analyser et de lui en rendre compte;

- de recommander à l'ÉHD les mesures à adopter pour traiter les risques et les exceptions à approuver;
- d'examiner et d'approuver la Politique sur la gestion des risques de TI et les normes afférentes.

Nous avons en outre noté que les Services de soutien aux activités (SSA) sont expressément responsables des tâches suivantes en ce qui a trait au programme de gestion des risques de la Ville :

- jouer le rôle d'agent de liaison entre la DST et leur direction générale dans les secteurs de la GRTI;
- communiquer les risques potentiels de TI à la DST pour les intégrer dans le registre des risques de TI pour l'ensemble de la Ville;
- participer à la fonction d'analyse des risques et au déroulement de l'évaluation annuelle des risques de TI de l'entreprise et y apporter son concours;
- communiquer les résultats de l'analyse des risques de TI dans le cadre des activités de gestion des risques de la direction générale;
- les SSA de la DGSO jouent également le rôle d'agent de liaison entre les unités des SSA des directions générales dans le cadre du processus d'évaluation et de regroupement des risques de TI.

Les SSA sont désormais chargés de dépister et de faire connaître les risques potentiels de TI et de participer à l'évaluation des risques; dans bien des cas, le personnel les désigne sous l'appellation de « praticiens des risques »; or, les personnes-ressources des SSA n'ont pas les connaissances technologiques ni la formation rigoureuse dans la gestion des risques pour pouvoir s'acquitter de ces responsabilités.

Compte tenu de ce qui précède, les rôles et les responsabilités sont définis plus clairement depuis qu'on a adopté le Cadre de GRTI. La Ville a apporté d'autres améliorations, en établissant des lignes directrices sur l'appétence et la tolérance au risque, notamment en réunissant 53 risques pour les secteurs d'activité et en adoptant un processus officialisé d'exemption des risques.

Nous avons toutefois 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 se rapportant aux approbations à délivrer pour les exemptions et les exceptions au titre des procédures uniformisées, ce qui a aussi une incidence sur la gouvernance et sur la surveillance des risques de TI.

Le *Cadre de gestion des risques de TI* (daté du 18 janvier 2018) précise que :

- l'équipe de la GRST doit recommander à l'ÉHD le traitement des risques et les exceptions à y apporter;
- l'Équipe de la haute direction est chargée d'approuver toutes les exceptions à apporter à la politique ou aux procédures.

La *Politique sur la sécurité de l'information* (datée du 16 juillet 2018) indique que le chef de l'information et le chef de la direction générale qui demande l'exemption (ou son fondé de pouvoir) doivent approuver les exemptions à apporter aux politiques sur la sécurité de l'information.

Le *Processus d'exemption au titre des risques de la sécurité technique* (daté du 7 septembre 2018) précise qu'il faut demander des approbations en fonction du risque évalué, à savoir :

- risque faible : approbation ou refus du gestionnaire de programme (GP) de la Sécurité des technologies (ST);
- risque moyen : approbation ou refus du chef de l'information des services de technologie de l'information;
- risque élevé : approbation ou refus de l'équipe de la Gestion des risques de sécurité des technologies (GRST).

Comme le démontre l'exposé ci-dessus, 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 constaté que les exemptions examinées (par exemple, une exemption pour un module complémentaire 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'avaient pas été approuvées par l'équipe de la haute direction ni par l'équipe de la GRST et qu'elles avaient été plutôt 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, 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 GRST et de l'équipe de la haute direction. En outre, nous avons noté que l'exemption qui autorisait l'archivage, aux États-Unis, renseignement 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, et nous invitons à la Ville à se pencher sur les enjeux potentiels liés à cette pratique.

Nous avons aussi noté que la Ville a commencé à mettre au point un processus annuel de validation des risques technologiques. Au moment de notre vérification, ce processus était toujours en voie d'élaboration. En raison de l'envergure et de la complexité des initiatives de gestion des risques, la Ville devrait se demander s'il faut consacrer d'autres ressources aux fonctions de gestion des risques de TI.

Répercussions :

L'absence de gouvernance en bonne et due forme pourrait limiter la possibilité, pour la haute direction, de connaître exactement les risques importants liés à la TI et le succès remporté par la Ville pour se prémunir contre ces risques. Les pratiques de gouvernance appropriées viennent aussi promouvoir une culture de sensibilisation aux risques permettent de prendre des décisions en fonction des risques. Des pratiques de gouvernance impropres peuvent donner lieu à des erreurs ou à des retards dans le dépistage des risques essentiels de TI pour la Ville et pourraient amener cette dernière à prendre des risques sans connaître parfaitement la nature potentielle ou la gravité éventuelle des conséquences.

Recommandation nº 2

Tableau 3 : Avancement

Mise à jour de la direction	Évaluation du BVG
Achevée	Partiellement achevée

Recommandation de la vérification :

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 initiale 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 deuxième trimestre de 2016.

Mise à jour de la direction :

Le trésorier municipal et le chef de l’information ont travaillé à l’établissement d’un modèle de budgétisation et de financement qui permet de financer les risques jugés inadmissibles.

Ce modèle prévoit :

- Un budget de dépenses en immobilisations accru pour les Services de technologie de l’information (STI), afin de tenir compte du cycle de vie des composants essentiels de l’infrastructure technologique. La majoration du financement a été approuvée dans le cadre du budget de 2016. Tous les fonds excédentaires seraient réaffectés aux directions générales de soutien qui n’ont

pas de budget de dépenses en immobilisations pour financer leur infrastructure technologique à risque élevé.

- L'établissement du cycle de vie de cinq ans pour les postes de travail et les ordinateurs portatifs et le financement du cycle de vie grâce aux comptes d'exploitation existants des STI. On a procédé à la mise en œuvre dans le cadre de l'examen annuel interne du budget des STI.
- L'établissement du financement nécessaire pour donner suite aux recommandations des vérificateurs dans le cadre de la Vérification 2015 de la gestion des risques de TI et de la Vérification de 2015 de la gestion des incidents de sécurité des TI et des interventions connexes afin d'améliorer, dans l'ensemble, la posture de sécurité de l'information et de cybersécurité à la Ville d'Ottawa.

Évaluation du BVG :

On a évalué les mesures décrites dans la mise à jour de la direction, et l'on a jugé qu'elles sont partiellement achevées.

Nous avons noté que les STI ont élaboré un plan stratégique triennal en 2017[2]. Ce plan vise à réaliser, d'ici 2020, les objectifs suivants :

- permettre aux clients d'avoir accès aux outils et à l'information n'importe quand, n'importe où et sur n'importe quel terminal;
- promouvoir l'efficience opérationnelle, en leur permettant de s'adapte à une croissance fulgurante et à une évolution rapide;
- mettre au point et appuyer les outils et les pratiques de pointe dans le domaine des technologies afin de permettre à la Ville de réaliser ses priorités opérationnelles;
- offrir aux clients des infrastructures et des outils sécuritaires, modernes et fiables pour répondre à leurs besoins opérationnels.

[2] Plan stratégique des STI 2018-2020.pdf

Pour atteindre ces objectifs, nous avons noté que les STI ont consigné par écrit un certain nombre d'initiatives qu'ils mèneront à bien, à savoir :

- créer et maintenir, pour la Ville, un environnement de sécurité « supérieur »;
- s'assurer que tous les actifs de technologie de l'information sont protégés comme il se doit, dans un paysage de sécurité qui ne cesse d'évoluer;
- adapter aux besoins de l'organisme l'utilisation des technologies à grande disponibilité (GD);
- mettre au point les pratiques de gestion des services de TI (par exemple, le contrôle des modifications et la prestation des services) afin d'optimiser l'investissement des ressources;
- améliorer et moderniser l'infrastructure des applications;
- activer les fonctions nouvelles et avancées de SAP.

Conformément aux initiatives de dépenses de TI à jour, le chef de l'information a institué un nouveau processus de prise en charge des projets des STI. Les analystes des opérations des TI travaillent en collaboration avec les groupes clients pour déterminer si un projet est d'envergure moindre ou considérable en faisant appel à une liste succincte de questions élémentaires permettant de définir le périmètre de l'intervention. Les projets de moindre envergure sont mis en œuvre dans le cycle de vie des projets lorsque les ressources sont réunies. Les projets de grande envergure doivent donner lieu à une discussion générale sur l'examen et les ressources avec une sous-équipe de cadres supérieurs avant d'enchaîner avec l'analyse de rentabilisation détaillée. Les STI coordonnent l'établissement de l'analyse de rentabilisation détaillée avec le concours de toutes les directions générales compétentes, notamment en tenant compte des besoins opérationnels détaillés fournis par le client. Le Comité directeur est chargé d'examiner l'analyse de rentabilisation et de gérer l'orientation du projet.

Nous avons noté que le plan des STI porte essentiellement sur les dépenses en immobilisations, de même que sur l'élaboration et la mise à jour des processus essentiels, 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 xxxx, ce qui indique que le financement des risques opérationnels de TI n'a peut-être pas suivi le rythme voulu.

Pendant les entrevues avec les STI, le BVG a appris que les STI n'ont pas considérablement redressé le budget opérationnel de la Ville chaque année pour pouvoir mettre l'accent sur leurs effectifs et que l'embauche de nouveaux employés auprès des STI est restée statique pendant un certain nombre d'années. En outre, de nombreux membres de l'équipe des STI ont noté que l'organisme n'a pas d'employés expérimentés pour mener à bien la plupart des projets décrits dans le plan stratégique des STI de la Ville.

Répercussions :

Pour maîtriser les risques de TI auxquels on a attribué des priorités dans l'ensemble de l'administration municipale, il faut compter sur le financement des immobilisations et des opérations, et il est essentiel de compter sur des ressources humaines expérimentées et en nombre suffisant pour maîtriser efficacement les risques de TI.

Recommandation nº 3

Tableau 4 : Avancement

Mise à jour de la direction	Évaluation du BVG
Achevée	Partiellement achevée

Recommandation de la vérification :

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 initiale de la direction :

La direction est d'accord avec cette recommandation.

Le directeur municipal, de concert avec les 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.

Mise à jour de la direction :

L'équipe de la gouvernance de la gestion de la sécurité des technologies (GRST) a été mise sur pied au quatrième trimestre de 2017; il s'agit d'un organisme de surveillance pour la maîtrise des risques et les décisions à prendre. Cette équipe a le pouvoir de formuler et d'approuver les recommandations portant sur les systèmes qui sont connectés à l'environnement général de TI de la Ville ou qui ont des incidences sur cet environnement, notamment tous les environnements de TI exploités indépendamment par une direction générale ou un comité.

Évaluation du BVG :

Nous avons évalué les mesures décrites dans la mise à jour de la direction, et nous avons jugé qu'elles sont partiellement achevées.

Nous avons noté que la Ville a mis sur pied l'équipe de la gestion des risques de sécurité des technologies (GRST). Cette équipe est responsable des activités suivantes :

- la gestion continue des programmes d'après le registre des risques de TI, le tableau de bord et l'évaluation annuelle des risques de TI;
- les questions dont elle est saisie par le chef de l'information et les changements ou les approbations portant sur l'ensemble des programmes;
- la hiérarchisation et le compte rendu des risques à l'intention de l'équipe de la haute direction;
- les recommandations à adresser à l'équipe de la haute direction sur le traitement des risques et sur les exceptions;
- l'examen et l'approbation de la Politique sur la gestion des risques de TI et des normes afférentes.

Comme nous l'expliquons dans les recommandations 1, 3, 4, 5, 6 et 7, 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 (ce qui influe sur la gouvernance et la surveillance des risques de TI).

Le *Cadre de gestion des risques de TI* (daté du 18 janvier 2018) précise que :

- l'équipe de la GRST est chargée d'adresser, à l'équipe de la haute direction, des recommandations sur le traitement des risques et les exceptions;
- l'équipe de la haute direction est chargée d'approuver toutes les exceptions à apporter à la politique ou aux procédures.

La *Politique sur la sécurité de l'information* (datée du 16 juillet 2018) indique que le chef de l'information et le chef de la direction générale qui demande l'exemption (ou son fondé de pouvoir) doivent approuver les exemptions à apporter aux politiques sur la sécurité de l'information.

Le *Processus d'exemption au titre des risques de la sécurité technique* (daté du 7 septembre 2018) précise qu'il faut demander des approbations en fonction du risque évalué, à savoir :

- risque faible : approbation ou refus du gestionnaire de programme (GP) de la Sécurité des technologies (ST);
- risque moyen : approbation ou refus du chef de l'information des services de technologie de l'information;
- risque élevé : approbation ou refus de l'équipe de la Gestion des risques de sécurité des technologies (GRST).

Comme le démontre l'exposé ci-dessus, 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 constaté que les exemptions examinées (par exemple, une exemption pour un module complémentaire 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'avaient pas été approuvées par l'équipe de la haute direction ni par l'équipe de la GRST et qu'elles avaient été plutôt 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, 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 GRST et de l'équipe de la haute direction. En outre, nous avons noté que l'exemption qui autorisait l'archivage, aux États-Unis, renseignement 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, et nous invitons à la Ville à se pencher sur les enjeux potentiels liés à cette pratique.

Répercussions :

L’absence de gouvernance en bonne et due forme pourrait limiter la possibilité, pour la haute direction, de connaître exactement les risques importants liés à la TI et le succès remporté par la Ville pour se prémunir contre ces risques. Les pratiques de gouvernance appropriées viennent aussi promouvoir une culture de sensibilisation aux risques permettent de prendre des décisions en fonction des risques. Des pratiques de gouvernance impropres peuvent donner lieu à des erreurs ou à des retards dans le dépistage des risques essentiels de TI pour la Ville et pourraient amener cette dernière à prendre des risques sans connaître parfaitement la nature potentielle ou la gravité éventuelle des conséquences.

Recommandation nº 4

Tableau 5 : Avancement

Mise à jour de la direction	Évaluation du BVG
Partiellement achevée	Partiellement achevée

Recommandation de la vérification :

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 initiale 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.

Mise à jour de la direction :

La version révisée de la Politique sur la sécurité de l’information (PSI) a été approuvée et a été mise à jour sur Ozone. Le directeur général des Services organisationnels et la trésorière municipale doivent la diffuser dans l’ensemble de l’administration municipale.

Cette politique confirme le rôle et les pouvoirs du chef de l’information en ce qui a trait à l’ensemble des risques techniques et de sécurité technique de la Ville. Le Cadre de gestion des risques de TI approuvé et diffusé dans l’ensemble de l’administration municipale décrit dans leurs grandes lignes les pratiques exemplaires de la profession et les processus administratifs en place pour permettre de suivre et de gérer efficacement les risques techniques et de sécurité technique à la Ville.

Le lancement de ce projet a été retardé en raison du remaniement organisationnel de la fin de 2016. On s'attend à ce que ce projet soit achevé au quatrième trimestre de 2018.

Évaluation du BVG :

Nous avons examiné la version révisée de la Politique sur la sécurité de l'information (PSI), dont la dernière révision est datée du 16 juillet 2018. La PSI précise les rôles et les responsabilités se rapportant aux services de TI pour la Ville. Elle décrit notamment les rôles suivants :

- directeur municipal;
- chef de l'information (CI);
- chefs des directions générales;
- gestionnaire de la Sécurité des technologies;
- administrateurs des systèmes;
- employés.

Nous avons noté que la Ville a publié, le 18 janvier 2018, un Cadre de gestion des risques de TI consigné par écrit. Ce cadre, qu'on vient d'élaborer, divise la gouvernance des risques en quatre activités essentielles :

- la mobilisation des directions générales de la Ville dans la gestion des risques de TI dont elles sont responsables;
- l'examen des risques de TI à l'échelon hiérarchique voulu, selon les modalités décrites dans le Circuit de travail de la GRTI;
- l'approbation des plans d'action pour maîtriser les risques supérieurs aux seuils fixés;
- la mise à jour des politiques et des normes de la Ville pour la GRTI.

Nous avons examiné le Cadre de TI des risques de l'ISACA[3], dont la dernière version a été publiée en 2009, et nous avons noté que le cadre de gestion des risques de TI de la Ville a été élaboré conformément au cadre de l'ISACA, qui précise que les administrations doivent :

- établir et mettre à jour une analyse commune des risques, notamment en procédant à intervalles réguliers à l'évaluation des risques de TI;

[3] http ://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx

- proposer des seuils de tolérance aux risques de TI;
- approuver la tolérance aux risques de TI;
- harmoniser la politique sur les risques de TI;
- promouvoir une culture de sensibilisation aux risques de TI;
- promouvoir l'efficacité de la diffusion des risques de TI.

Nous avons noté que le cadre de la Ville s'harmonise avec le Cadre de gestion des risques de TI de l'ISACA. Nous avons noté que dans le cadre de la Ville, les STI interviennent dans les travaux d'examen des risques de TI, à l'échelon voulu, selon les modalités exposées dans le circuit de travail de la GRTI. Conformément à cette exigence, la Ville a commencé à mettre au point un processus annuel de validation des risques. On n'a toujours pas achevé l'élaboration de ce processus. Le processus de validation consiste à examiner les constatations des précédentes évaluations des menaces et des risques et à en faire état dans le registre des risques des STI. Lorsque les risques sont répertoriés, il faut procéder à une évaluation des menaces et des risques (ÉMR). Les STI espèrent que des membres de l'équipe de la sécurité de la TI effectueront cet examen. Les STI ont noté que le registre comprend environ 120 risques (à l'exception des six secteurs d'activité qui n'ont pas encore été examinés). On a noté, pendant les discussions avec les STI, que les Services de sécurité de la TI ont actuellement à leur service quatre employés à temps plein et qu'ils font appel à un entrepreneur pour mener les ÉMR. Compte tenu du nombre d'ÉMR à réaliser et du nombre de ressources disponibles, il sera difficile d'effectuer à temps les évaluations portant sur tous les risques, en tenant compte du fait que de nouveaux risques viennent s'ajouter chaque jour dans le registre.

Le personnel nous a fait savoir que les STI n'avaient pas suffisamment d'employés expérimentés et compétents pour mener à bien les ÉMR. C'est ce qui a été précisé lorsqu'on a noté qu'à l'origine, dans le cadre du contrôle de concordance des risques des 53 différents secteurs d'activité, les STI avaient prévu de réaliser un projet pilote portant sur un certain nombre de secteurs d'activité pour déterminer l'effort à consacrer à la captation des risques de TI. Dans la foulée du projet pilote mené auprès d'un secteur d'activité ou de deux secteurs, la direction a décidé que 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. 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.

Comme nous l'expliquons dans les recommandations 1, 3, 4, 5, 6 et 7, 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 (ce qui influe sur la gouvernance et la surveillance des risques de TI).

Le *Cadre de gestion des risques de TI* (daté du 18 janvier 2018) précise que :

- l'équipe de la GRST est chargée d'adresser, à l'équipe de la haute direction, des recommandations sur le traitement des risques et les exceptions;
- l'équipe de la haute direction est chargée d'approuver toutes les exceptions à apporter à la politique ou aux procédures.

La *Politique sur la sécurité de l'information* (datée du 16 juillet 2018) indique que le chef de l'information et le chef de la direction générale qui demande l'exemption (ou son fondé de pouvoir) doivent approuver les exemptions à apporter aux politiques sur la sécurité de l'information.

Le *Processus d'exemption au titre des risques de la sécurité technique* (daté du 7 septembre 2018) précise qu'il faut demander des approbations en fonction du risque évalué, à savoir :

- risque faible : approbation ou refus du gestionnaire de programme (GP) de la Sécurité des technologies (ST);
- risque moyen : approbation ou refus du chef de l'information des services de technologie de l'information;
- risque élevé : approbation ou refus de l'équipe de la Gestion des risques de sécurité des technologies (GRST).

Comme le démontre l'exposé ci-dessus, 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 constaté que les exemptions examinées (par exemple, une exemption pour un module complémentaire 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'avaient pas été approuvées par l'équipe de la haute direction ni par l'équipe de la GRST et qu'elles avaient été plutôt 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, 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 GRST et de l'équipe de la haute direction. En outre, nous avons noté que l'exemption qui autorisait l'archivage, aux États-Unis, renseignement 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, et nous invitons à la Ville à se pencher sur les enjeux potentiels liés à cette pratique.

Répercussions :

L'absence de gouvernance en bonne et due forme pourrait limiter la possibilité, pour la haute direction, de connaître exactement les risques importants liés à la TI et le succès remporté par la Ville pour se prémunir contre ces risques. Les pratiques de gouvernance appropriées viennent aussi promouvoir une culture de sensibilisation aux risques permettent de prendre des décisions en fonction des risques. Des pratiques de gouvernance impropres peuvent donner lieu à des erreurs ou à des retards dans le dépistage des risques essentiels de TI pour la Ville et pourraient amener cette dernière à prendre des risques sans connaître parfaitement la nature potentielle ou la gravité éventuelle des conséquences.

Recommandation nº 5

Tableau 6 : Avancement

Mise à jour de la direction	Évaluation du BVG
Partiellement achevée	Partiellement achevée

Recommandation de la vérification :

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);
- définit 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;
- 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.

Réponse initiale 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.

Mise à jour de la direction :

Le Cadre de gestion des risques de TI (GRTI) a été approuvé et diffusé dans l'ensemble de l'administration municipale. Ce document décrit dans leurs grandes lignes les rôles de la haute direction et la gouvernance des risques techniques et de sécurité technique à la Ville. Il s'agit notamment d'un processus rigoureux d'exemption des risques et de l'équipe mise sur pied pour la gouvernance de la gestion des risques de sécurité technique (GRST), ainsi que d'un processus annuel de validation des risques, dans le cadre duquel les priorités sont établies d'après les risques qui sont supérieurs aux seuils fixés.

Le Cadre de GRTI a été mis au point de concert avec le cadre actuel de GRE. Il existe un registre des risques opérationnels, qui permet de suivre et de gérer les risques techniques et de sécurité technique et de suivre les mesures permettant de maîtriser les risques pour s'assurer que ces mesures sont appliquées. Le tableau de bord du registre des risques est produit pour l'ensemble des directions générales, des secteurs d'activité et de l'entreprise.

Le processus annuel de validation des risques est en cours et sera achevé d'ici le quatrième trimestre de 2018.

Évaluation du BVG :

Nous avons évalué les mesures décrites dans la mise à jour de la direction et nous avons jugé qu'elles sont partiellement achevées.

Nous avons noté que la Ville a publié, le 18 janvier 2018, un cadre de gestion des risques de TI consigné par écrit. Ce cadre de gestion des risques de TI, qui vient d'être élaboré, définit la gouvernance des risques selon quatre activités essentielles :

- la mobilisation des directions générales de la Ville dans la gestion des risques de TI dont elles sont responsables;
- l'examen des risques de TI à l'échelon hiérarchique voulu, selon les modalités décrites dans le Circuit de travail de la GRTI;
- l'approbation des plans d'action pour maîtriser les risques supérieurs aux seuils fixés;
- la mise à jour des politiques et des normes de la Ville pour la GRTI.

Ce cadre définit aussi les rôles de la haute direction et la gouvernance des risques techniques et de sécurité technique de la Ville. Il s'agit notamment :

- de l'équipe de la haute direction, qui est responsable de l'ensemble du programme de GRTI;
- de l'équipe de cadres de la direction générale, qui est responsable de la gestion des risques de TI et de sécurité de l'information dans sa propre direction générale;
- de l'Équipe de gestion des risques pour la sécurité des technologies, qui assure la gouvernance opérationnelle du programme de GRTI, notamment la hiérarchisation et l'approbation des exceptions;
- du chef de l'information, qui doit rendre des comptes à l'équipe de la GRST dans la gestion du programme de GRTI et qui assume la responsabilité de la GRTI de l'ensemble de l'infrastructure partagée de TI gérée par les STI;
- de la Direction de la sécurité des technologies (DST), qui est fonctionnellement responsable de nombreux volets du programme de GRTI;
- des Services de soutien aux activités (SSA), qui sont le point de contact, dans les directions générales, pour toutes les activités de gestion des risques.

Nous avons noté que le cadre qu'on vient d'élaborer s'harmonise avec le cadre de gestion des risques de l'entreprise (GRE) existant de la Ville. On n'a pas défini le répertoire complet du périmètre de TI pour l'ensemble de la Ville (applications, responsables opérationnels, réseaux et liens de dépendance, entre autres), qui constituerait un point de départ pour analyser et recenser les risques de TI. Il existe un registre des risques opérationnels, qui sert à faire connaître les risques en faisant appel à un tableau de bord. Nous avons constaté qu'un récent examen trimestriel avait été effectué sous le titre « Aperçu trimestriel du Registre des risques de sécurité des technologies », en date d'octobre 2018.

Nous avons noté que les Services de soutien aux activités (SSA) sont expressément responsables des tâches suivantes en ce qui a trait au programme de gestion des risques de la Ville :

- jouer le rôle d'agent de liaison entre la DST et leur direction générale dans les secteurs de la GRTI;
- communiquer les risques potentiels de TI à la DST pour les intégrer dans le registre des risques de TI pour l'ensemble de la Ville;

- participer à la fonction d'analyse des risques et au déroulement de l'évaluation annuelle des risques de TI de l'entreprise et y apporter son concours;
- communiquer les résultats de l'analyse des risques de TI dans le cadre des activités de gestion des risques de la direction générale;
- les SSA de la DGSO jouent également le rôle d'agent de liaison entre les unités des SSA des directions générales dans le cadre du processus d'évaluation et de regroupement des risques de TI.

Les SSA sont désormais chargés de dépister et de faire connaître les risques potentiels de TI et de participer à l'évaluation des risques; dans bien des cas, le personnel les désigne sous l'appellation de « praticiens des risques »; or, les personnes-ressources des SSA n'ont pas les connaissances technologiques ni de formation rigoureuse dans la gestion des risques pour pouvoir s'acquitter de ces responsabilités.

En outre, nous avons noté que l'Équipe de la gestion des risques de la sécurité des technologies (GRST) est constituée :

- du directeur général de la Direction générale des services organisationnels (DGSO);
- du greffier municipal et avocat général;
- du chef de l'information.

L'Équipe de la GRST est responsable :

- de la gestion permanente des programmes d'après le registre des risques de TI, le tableau de bord et l'évaluation des risques de TI;
- de se pencher sur les questions portées à son attention par le chef de l'information et sur les changements ou les approbations dans l'ensemble du programme;
- de saisir l'équipe de la haute direction (ÉHD) des risques à analyser et de lui en rendre compte;
- de recommander à l'ÉHD les mesures à adopter pour traiter les risques et les exceptions à approuver;
- d'examiner et d'approuver la Politique sur la gestion des risques de TI et les normes afférentes.

Comme nous l'expliquons dans les recommandations 1, 3, 4, 5, 6 et 7, 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 (ce qui influe sur la gouvernance et la surveillance des risques de TI, ainsi que sur le rôle, la responsabilité et l'imputabilité attribuable au poste de chef de l'information).

Le *Cadre de gestion des risques de TI* (daté du 18 janvier 2018) précise que :

- l'équipe de la GRST est chargée d'adresser, à l'équipe de la haute direction, des recommandations sur le traitement des risques et les exceptions;
- l'équipe de la haute direction est chargée d'approuver toutes les exceptions à apporter à la politique ou aux procédures.

La *Politique sur la sécurité de l'information* (datée du 16 juillet 2018) indique que le chef de l'information et le chef de la direction générale qui demande l'exemption (ou son fondé de pouvoir) doivent approuver les exemptions à apporter aux politiques sur la sécurité de l'information.

Le *Processus d'exemption au titre des risques de la sécurité technique* (daté du 7 septembre 2018) précise qu'il faut demander des approbations en fonction du risque évalué, à savoir :

- risque faible : approbation ou refus du gestionnaire de programme (GP) de la Sécurité des technologies (ST);
- risque moyen : approbation ou refus du chef de l'information des services de technologie de l'information;
- risque élevé : approbation ou refus de l'équipe de la Gestion des risques de sécurité des technologies (GRST).

Comme le démontre l'exposé ci-dessus, 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 constaté que les exemptions examinées (par exemple, une exemption pour un module complémentaire 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'avaient pas été approuvées par l'équipe de la haute direction ni par l'équipe de la GRST et qu'elles avaient été plutôt 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, 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 GRST et de l'équipe de la haute direction. En outre, nous avons noté que l'exemption qui autorisait l'archivage, aux États-Unis, renseignement 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, et nous invitons à la Ville à se pencher sur les enjeux potentiels liés à cette pratique.

Répercussions :

L'absence de gouvernance en bonne et due forme pourrait limiter la possibilité, pour la haute direction, de connaître exactement les risques importants liés à la TI et le succès remporté par la Ville pour se prémunir contre ces risques. Les pratiques de gouvernance appropriées viennent aussi promouvoir une culture de sensibilisation aux risques permettent de prendre des décisions en fonction des risques. Des pratiques de gouvernance impropres peuvent donner lieu à des erreurs ou à des retards dans le dépistage des risques essentiels de TI pour la Ville et pourraient amener cette dernière à prendre des risques sans connaître parfaitement la nature potentielle ou la gravité éventuelle des conséquences.

Recommandation nº 6

Tableau 7 : Avancement

Mise à jour de la direction	Évaluation du BVG
Partiellement achevée	Partiellement achevée

Recommandation de la vérification :

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 initiale de la direction :

La direction est d’accord avec cette recommandation.

Elle mettra au point des politiques et des procédures pour doter le cadre de la GRTI des mécanismes d’analyse voulus. On définira les compétences nécessaires et la formation à prévoir, dont on tiendra compte dans la mise en œuvre du cadre. Cette recommandation sera achevée d’ici le quatrième trimestre de 2017.

Mise à jour de la direction :

Le PSI révisé et approuvé confirme le rôle et les pouvoirs du chef de l’information en ce qui a trait à l’ensemble des risques techniques et de sécurité technique à la Ville.

À l’heure actuelle, on consigne par écrit le processus annuel de validation des risques (qui fait partie du cadre de gestion des risques), qui dépend des processus d’évaluation des risques exécutés par les personnes-ressources techniques compétentes pour l’ensemble des modifications techniques. Les STI travaillent de concert avec les unités des Services de soutien aux activités pour finaliser les processus annuels de validation des risques.

Il y a eu un retard dans le lancement du projet en raison du remaniement organisationnel de 2016. On s'attend à ce que ce travail soit achevé au quatrième trimestre de 2018.

Évaluation du BVG :

Nous avons noté que la Ville a commencé à mettre au point un processus annuel de validation des risques technologiques. Au moment de notre vérification, ce processus était toujours en voie d'élaboration. En raison de l'envergure et de la complexité des initiatives de gestion des risques, la Ville devrait envisager de mieux répartir les ressources nécessaires pour exercer les fonctions de gestion des risques de TI.

Nous avons noté que les Services de soutien aux activités (SSA) sont expressément responsables des tâches suivantes en ce qui a trait au programme de gestion des risques de la Ville :

- jouer le rôle d'agent de liaison entre la DST et leur direction générale dans les secteurs de la GRTI;
- communiquer les risques potentiels de TI à la DST pour les intégrer dans le registre des risques de TI pour l'ensemble de la Ville;
- participer à la fonction d'analyse des risques et au déroulement de l'évaluation annuelle des risques de TI de l'entreprise et y apporter son concours;
- communiquer les résultats de l'analyse des risques de TI dans le cadre des activités de gestion des risques de la direction générale;
- les SSA de la DGSO jouent également le rôle d'agent de liaison entre les unités des SSA des directions générales dans le cadre du processus d'évaluation et de regroupement des risques de TI.

Les SSA sont désormais chargés de dépister et de faire connaître les risques potentiels de TI et de participer à l'évaluation des risques; dans bien des cas, le personnel les désigne sous l'appellation de « praticiens des risques »; or, les personnes-ressources des SSA n'ont pas les connaissances technologiques ni la formation rigoureuse dans la gestion des risques pour pouvoir s'acquitter de ces responsabilités.

Comme nous l'expliquons dans les recommandations 1, 3, 4, 5, 6 et 7, 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 (ce qui influe sur la gouvernance et la surveillance des risques de TI).

Le *Cadre de gestion des risques de TI* (daté du 18 janvier 2018) précise que :

- l'équipe de la GRST est chargée d'adresser, à l'équipe de la haute direction, des recommandations sur le traitement des risques et les exceptions;
- l'équipe de la haute direction est chargée d'approuver toutes les exceptions à apporter à la politique ou aux procédures.

La *Politique sur la sécurité de l'information* (datée du 16 juillet 2018) indique que le chef de l'information et le chef de la direction générale qui demande l'exemption (ou son fondé de pouvoir) doivent approuver les exemptions à apporter aux politiques sur la sécurité de l'information.

Le *Processus d'exemption au titre des risques de la sécurité technique* (daté du 7 septembre 2018) précise qu'il faut demander des approbations en fonction du risque évalué, à savoir :

- risque faible : approbation ou refus du gestionnaire de programme (GP) de la Sécurité des technologies (ST);
- risque moyen : approbation ou refus du chef de l'information des services de technologie de l'information;
- risque élevé : approbation ou refus de l'équipe de la Gestion des risques de sécurité des technologies (GRST).

Comme le démontre l'exposé ci-dessus, 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 constaté que les exemptions examinées (par exemple, une exemption pour un module complémentaire 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'avaient pas été approuvées par l'équipe de la haute direction ni par l'équipe de la GRST et qu'elles avaient été plutôt 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, 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 GRST et de l'équipe de la haute direction. En outre, nous avons noté que l'exemption qui autorisait l'archivage, aux États-Unis, renseignement 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, et nous invitons à la Ville à se pencher sur les enjeux potentiels liés à cette pratique.

En outre, nous n'avons pas relevé de pièces justificatives confirmant que les ensembles de compétences et les spécifications de la formation pour les volets des documents sur la GRTI en ce qui concerne les directions générales ont été précisés.

Répercussions :

L'absence de gouvernance en bonne et due forme pourrait limiter la possibilité, pour la haute direction, de connaître exactement les risques importants liés à la TI et le succès remporté par la Ville pour se prémunir contre ces risques. Les pratiques de gouvernance appropriées viennent aussi promouvoir une culture de sensibilisation aux risques permettent de prendre des décisions en fonction des risques. Des pratiques de gouvernance impropres peuvent donner lieu à des erreurs ou à des retards dans le dépistage des risques essentiels de TI pour la Ville et pourraient amener cette dernière à prendre des risques sans connaître parfaitement la nature potentielle ou la gravité éventuelle des conséquences.

Recommandation nº 7

Tableau 8 : Avancement

Mise à jour de la direction	Évaluation du BVG
Achevée	Partiellement achevée

Recommandation de la vérification :

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 initiale 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.

Mise à jour de la direction :

Le cadre de gestion des risques de TI (GRTI) a été approuvé et diffusé dans l'ensemble de l'administration municipale.

Les processus auxiliaires décrivent dans leurs grandes lignes les méthodologies, les modèles et les outils, ainsi que les rôles et les responsabilités dans l'évaluation des risques et permettent de suivre ces risques et les mesures d'atténuation pour toutes les modifications technologiques. Il s'agit notamment d'un processus formel d'exemption des risques et de l'équipe de gouvernance mise sur pied pour la gestion des risques de

sécurité technique (GRST), ainsi que d'un processus annuel de validation des risques, dans lequel les priorités sont établies en fonction des risques qui sont supérieurs aux seuils fixés.

À l'heure actuelle, on consigne par écrit le processus annuel de validation des risques, avec le concours des unités des Services de soutien aux activités.

Évaluation du BVG :

Nous avons examiné la Politique sur la sécurité de l'information (PSI), dont la dernière révision remonte au 16 juillet 2018. La PSI précise les rôles et les responsabilités en ce qui a trait aux services de TI de la Ville. Cette politique décrit notamment les rôles suivants :

- directeur municipal;
- chef de l'information (CI);
- chefs des directions générales;
- gestionnaire de la Sécurité des technologies;
- administrateurs des systèmes;
- employés.

Nous avons noté que la Ville a publié, le 18 janvier 2018, un Cadre de gestion des risques de TI consigné par écrit. Ce cadre, qu'on vient d'élaborer, divise la gouvernance des risques en quatre activités essentielles :

- la mobilisation des directions générales de la Ville dans la gestion des risques de TI dont elles sont responsables;
- l'examen des risques de TI à l'échelon hiérarchique voulu, selon les modalités décrites dans le Circuit de travail de la GRTI;
- l'approbation des plans d'action pour maîtriser les risques supérieurs aux seuils fixés;
- la mise à jour des politiques et des normes de la Ville pour la GRTI.

Nous avons examiné le Cadre de TI des risques de l'ISACA [4], dont la dernière version a été publiée en 2009, et nous avons noté que le cadre de gestion des risques de TI de la

[4] http ://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx

Ville a été élaboré conformément au cadre de l'ISACA, qui précise que les administrations doivent :

- établir et mettre à jour une analyse commune des risques, notamment en procédant à intervalles réguliers à l'évaluation des risques de TI;
- proposer des seuils de tolérance aux risques de TI;
- approuver la tolérance aux risques de TI;
- harmoniser la politique sur les risques de TI;
- promouvoir une culture de sensibilisation aux risques de TI;
- promouvoir l'efficacité de la diffusion des risques de TI.

Nous avons noté que le cadre de la Ville s'harmonise avec le Cadre de TI des risques de ISACA. Nous avons noté que dans le cadre de la Ville, les STI participent au travail qui consiste à examiner les risques de TI, à l'échelon voulu, selon les modalités exposées dans le circuit de travail de la GRTI.

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.

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.

En raison de l'envergure et de la complexité des initiatives de gestion des risques, la Ville devrait envisager de mieux répartir les ressources nécessaires pour exercer les fonctions de gestion des risques de TI.

Comme nous l'expliquons dans les recommandations 1, 3, 4, 5, 6 et 7, 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 (ce qui influe sur la gouvernance et la surveillance des risques de TI, ainsi que sur le rôle, la responsabilité et l'imputabilité attribuable au poste de chef de l'information).

Le *Cadre de gestion des risques de TI* (daté du 18 janvier 2018) précise que :

- l'équipe de la GRST est chargée d'adresser, à l'équipe de la haute direction, des recommandations sur le traitement des risques et les exceptions;
- l'équipe de la haute direction est chargée d'approuver toutes les exceptions à apporter à la politique ou aux procédures.

La *Politique sur la sécurité de l'information* (datée du 16 juillet 2018) indique que le chef de l'information et le chef de la direction générale qui demande l'exemption (ou son fondé de pouvoir) doivent approuver les exemptions à apporter aux politiques sur la sécurité de l'information.

Le *Processus d'exemption au titre des risques de la sécurité technique* (daté du 7 septembre 2018) précise qu'il faut demander des approbations en fonction du risque évalué, à savoir :

- risque faible : approbation ou refus du gestionnaire de programme (GP) de la Sécurité des technologies (ST);
- risque moyen : approbation ou refus du chef de l'information des services de technologie de l'information;
- risque élevé : approbation ou refus de l'équipe de la Gestion des risques de sécurité des technologies (GRST).

Comme le démontre l'exposé ci-dessus, 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 constaté que les exemptions examinées (par exemple, une exemption pour un module complémentaire 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'avaient pas été approuvées par l'équipe de la haute direction ni par l'équipe de la GRST et qu'elles avaient été plutôt 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, 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 GRST et de l'équipe de la haute direction. En outre, nous avons noté que l'exemption qui autorisait l'archivage, aux États-Unis, renseignement 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, et nous invitons à la Ville à se pencher sur les enjeux potentiels liés à cette pratique.

Répercussions :

L’absence de gouvernance en bonne et due forme pourrait limiter la possibilité, pour la haute direction, de connaître exactement les risques importants liés à la TI et le succès remporté par la Ville pour se prémunir contre ces risques. Les pratiques de gouvernance appropriées viennent aussi promouvoir une culture de sensibilisation aux risques permettent de prendre des décisions en fonction des risques. Des pratiques de gouvernance impropres peuvent donner lieu à des erreurs ou à des retards dans le dépistage des risques essentiels de TI pour la Ville et pourraient amener cette dernière à prendre des risques sans connaître parfaitement la nature potentielle ou la gravité éventuelle des conséquences.

Recommandation nº 8

Tableau 9 : Avancement

Mise à jour de la direction	Évaluation du BVG
Achevée	Impossible à évaluer

Recommandation de la vérification :

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 initiale 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, les STI évalueront annuellement les nouvelles stratégies d’atténuation des risques.

Mise à jour de la direction :

On applique les principes de l’amélioration continuelle au cadre de gestion des risques de TI et aux processus auxiliaires. En outre, ce cadre et ces processus doivent être revus chaque année selon le processus annuel de validation des risques. Les objectifs et les résultats clés (ORC) de la Direction de la sécurité technique prévoient des examens annuels des outils et des méthodologies pour s’assurer qu’ils sont conformes aux pratiques exemplaires de la profession.

À l’heure actuelle, on consigne par écrit le processus annuel de validation des risques avec le concours des unités des Services de soutien aux activités.

Ce projet a été retardé en raison du remaniement organisationnel de 2016. On s’attend à ce qu’il soit achevé au quatrième trimestre de 2018.

Évaluation du BVG :

Le BVG a procédé à l’examen de la version 1.0 du document sur le Cadre de gestion des risques de TI (GRTI) qui a été publié le 28 janvier 2018. Nous avons noté que la section consacrée aux révisions indique seulement que le document a été approuvé le 17 janvier 2018. Puisque la stratégie n’est revue qu’une fois par an, le BVG n’a pas pu prendre connaissance des modifications et des améliorations apportées au Cadre de GRTI.

Tableau 10 : Légende des degrés d'achèvement

Achèvement	Définition
À venir	Aucun progrès tangible n'a été réalisé. L'élaboration de plans non officiels n'est pas considérée comme un progrès tangible.
Partiellement achevée	La Ville a entamé la mise en œuvre, mais celle-ci n'est pas encore terminée.
Achevée	La mesure a été prise, ou les structures et les processus fonctionnent comme il se doit et ont été entièrement adoptés dans tous les secteurs concernés de la Ville.
Impossible à évaluer	La mesure n'est pas appliquée à l'heure actuelle; la recommandation reste toutefois applicable.