Ottawa

Bureau de la vérificatrice générale

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 27 avril 2021

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 de 2020 du Bureau du vérificateur général.

Le précédent suivi de la vérification de la gestion des risques liés aux technologies de l'information, déposé le 29 mai 2019 auprès du Comité de la vérification, indiquait que sept des huit recommandations issues de la vérification de 2015 étaient partiellement achevées et qu'on n'avait pas pu évaluer, à l'époque, une recommandation. Par conséquent, on a ensuite inclus ce suivi dans le Plan de vérification de 2020 du Bureau du vérificateur général afin de revoir les huit recommandations.

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

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

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 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 des STI et des employés en dehors des 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 dans la gestion des risques liés aux TI de même dans 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 risques les plus importants liés aux TI se déroulent uniformément, correctement et assez rapidement. 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 huit constatations ont par la suite toutes été évaluées dans le cadre de cette vérification. Les détails de cette évaluation sont compris dans le rapport détaillé.

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

Recommandation	État en date de décembre 2018	État selon la direction en date d'août 2020	État selon le BVG en date de novembre 2020
Nº 1	Partiellement achevée	Achevée	Achevée
Nº 2	Partiellement achevée	Achevée	Achevée
Nº 3	Partiellement achevée	Achevée	Achevée
Nº 4	Partiellement achevée	Achevée	Achevée
Nº 5	Partiellement achevée	Achevée	Achevée
Nº 6	Partiellement achevée	Achevée	Achevée
Nº 7	Partiellement achevée	Achevée	Achevée
Nº 8	Impossible à évaluer	Achevée	Achevée
Total	**7 partiellement achevée (88 %)** **1 impossible à évaluer**	**8 achevées** **(100 %)**	**8 achevées** **(100 %)**

Conclusion

Depuis notre précédent suivi, en 2018, la direction a achevé les huit recommandations. Le processus de la GRST se situe désormais à l'étape de la version 2.0; on y a apporté d'autres améliorations, et le processus cadre mieux avec celui de la gestion des risques de l'entreprise. On a aussi mené le processus de validation annuelle de gestion des risques de TI pour assurer la vérification complémentaire des risques de TI « absolument prioritaires ».

Bien que nous ayons constaté que la direction s'était penchée sur tous les secteurs dans lesquels nous avons fait des observations auparavant, nous avons relevé des cas mineurs dans lesquels on pourrait améliorer encore les contrôles exercés dans certains secteurs, notamment l'officialisation des décisions dans la gestion des risques et le contrôle complémentaire de la concordance des stratégies de maîtrise des risques.

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 2.0, le processus d’exemption des risques, le processus de validation annuelle de validation des risques de la GRTI et la Politique sur la sécurité de l’information, entre autres.

Les vérificateurs ont également tenu des 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 et le directeur, Sécurité de l’information et Gestion des risques numériques.

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 2020, ainsi que l’évaluation du Bureau du vérificateur général (BVG) en date de novembre 2020.

Recommandation nº 1

Tableau 2 : Avancement

Mise à jour de la direction	Évaluation du BVG
Achevée	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 les Services 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 en août 2020 :

Afin de corriger les incohérences relevées par le BVG dans le rapport de suivi, les STI ont mis à jour la Politique sur la sécurité de l'information (PSI), le Cadre de gestion des risques de TI (GRTI) et la Politique de gestion des risques d'entreprise (PGRE) afin

d'harmoniser les rôles et les responsabilités dans l'ensemble des politiques. Il s'agit entre autres des critères et des exemples se rapportant aux pouvoirs d'approbation et de l'institution d'un processus de validation annuelle des risques.

L'équipe de la gouvernance de la Gestion des risques de la sécurité technique (GRST) a été mise sur pied en juillet 2017 pour encadrer la GRTI.

Le processus de validation annuelle des risques a été réalisé dans l'ensemble de l'administration municipale en janvier 2020. Toutes les évaluations des risques et tous les travaux de validation des risques ont été menés par les membres compétents de l'équipe de la Sécurité de la technologie. La Direction de la sécurité des technologies a investi dans la formation et dans la certification du personnel.

L'équipe de gestion des TI a créé le nouveau poste de directeur, Sécurité de l'information et Gestion des risques numériques (DSIGRN), qui relève directement de la directrice générale de la Direction générale des services novateurs pour la clientèle. Le titulaire de ce poste est responsable du perfectionnement du programme actuel de sécurité, ainsi que de la mise au point d'une approche stratégique pour l'amélioration continuelle.

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 achevées.

Le BVG a appris que la GAR est gérée selon un certain niveau de tolérance au risque. On se penche sur les risques faibles quand l'environnement des risques constituant des menaces évolue. On a apporté des changements dans la définition des risques dans le cadre de la pandémie de COVID.

Nous avons constaté que la Ville a produit la version 2.0 à jour du document portant sur le Cadre de gestion des risques de TI le 13 décembre 2019. Le document à jour cadre désormais mieux avec la Politique de gestion des risques d'entreprise (PGRE) et fait état des rôles et des responsabilités de l'équipe de la Gestion des risques de sécurité des technologies (GRST), du chef de l'information, de l'équipe de dirigeants de la Direction générale, de la Direction de la sécurité des technologies (DST) et des Services de soutien aux activités.

Les cotes des risques sont calculées selon la cartographie des risques 5x5, qui cadre avec la PGRE. On a constaté que les risques faibles (dont la cote est comprise entre 1 et 4) ne sont pas suivis. Le chef de l'information peut approuver les risques dont la cote est comprise entre 5 et 12, et l'équipe de la GRST doit approuver ceux dont la cote est comprise entre 15 et 25.

Pour les activités liées à la maîtrise des risques, on ouvre des bons de travail dans le système de demandes de bons Marval et on les confie aux secteurs compétents. L'aspect relatif à la planification des opérations fait partie de l'ensemble du processus, et les éléments qui réclament l'attention des responsables sont définis comme des éléments prioritaires.

Conformément au Cadre de gestion des risques de l'entreprise, toutes les directions générales doivent gérer leurs risques, y compris ceux qui sont répertoriés dans le Registre et le Tableau de bord des risques de TI.

Le BVG a appris que le gestionnaire du soutien stratégique, Service novateur pour la clientèle gère les risques d'entreprise dans un tableur, qui est établi à partir du Plan de TI. Nous avons constaté que le contrôle de concordance des stratégies de maîtrise des risques paraît limité et la direction devrait se pencher sur de nouvelles activités de contrôle de concordance afin de continuer d'apporter des améliorations à cet égard.

Recommandation nº 2

Tableau 3 : Avancement

Mise à jour de la direction	Évaluation du BVG
Achevée	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 les Services 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 2018:

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.

Mise à jour de la direction en août 2020 :

- La direction des TI a examiné le budget actuel afin de s'assurer qu'elle dispose du financement qui lui permettra de maîtriser les risques priorisés. Le budget opérationnel de la sécurité des TI et des risques correspondants a été augmenté d'environ 80 % dans la période comprise entre 2018 et 2020.
- On a créé le « Fonds de renouvellement des TI » en faisant appel à des dépenses en immobilisations pour financer une sélection de projets de technologie jugés prioritaires pour l'administration municipale, notamment les projets qui permettent aux STI de gérer efficacement et proactivement les risques de sécurité de l'administration municipale. Ce fonds est géré par le chef de l'information, qui travaille de concert avec la Direction générale des services des finances pour dresser chaque année la liste des projets, établir un plan de dépenses général et préparer un plan budgétaire pour répondre aux impératifs opérationnels correspondants.
- La Direction de la sécurité technologique a aussi enrichi son effectif de trois postes, dont un responsable spécialisé pour la fonction de gestion des risques de sécurité.

On a créé, au sein de l'équipe de la direction des TI, le nouveau poste de directeur, Sécurité de l'information et Gestion des risques numériques, qui relève directement

de la directrice générale de la Direction générale des services novateurs pour la clientèle. Le titulaire de ce poste doit s’assurer que la gestion des risques est à la fois intégrée et maximisée afin de prendre de meilleures décisions dans la gestion des risques au sein de l’administration municipale. Il doit également assurer l’amélioration continuelle du programme de gestion des risques pour la sécurité.

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 achevées.

Nous avons examiné le tableau comparatif des budgets sur trois ans de la Direction de la sécurité technologique et avons constaté que ce budget a augmenté pour passer de 2,315 M$ en 2018 à 4,197 M$ en 2020. Entre autres, les « services achetés » ont augmenté pour passer de 65 737 $ à plus de 900 000 $ en 2019 et en 2020 à la fois. La création du poste de directeur, Sécurité de l’information et Gestion des risques numériques et le recrutement d’un responsable d’expérience mettent en lumière la volonté d’améliorer la situation et d’engager des dépenses ciblées dans le domaine des TI, tout en apportant les compétences supplémentaires signalées comme des lacunes auparavant dans la gestion de la sécurité et des risques.

Recommandation nº 3

Tableau 4 : Avancement

Mise à jour de la direction	Évaluation du BVG
Achevée	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 en 2018 :

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.

Mise à jour de la direction en août 2020 :

Veuillez consulter la réponse apportée à la recommandation 1.

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 achevées.

On a créé dans Microsoft Teams un canal consacré à la GRST à l’intention des membres de l’organisme de gouvernance de la GRST; ce canal est désormais utilisé pour tenir les discussions sur les risques et pour enregistrer et consigner les approbations. La direction a fourni la preuve de cinq cas distincts dans lesquels on a discuté des risques sur la chaîne de Teams. Il s’agit entre autres d’un certain nombre d’exceptions se rapportant à la COVID-19 et de la connectivité à assurer pour le télétravail.

La direction a fait savoir qu’à son avis, « la chaîne de Teams est un moyen efficace et efficient d’avoir des échanges sur le mandat de la gouvernance de la GRST, surtout dans la foulée du scénario de télétravail forcé en réaction à la pandémie mondiale. Le mandat approuvé fait état de cette plateforme de réunion ». La direction prévoit aussi de préciser que cette méthode de consultation est « la méthode privilégiée pour les évaluations types des risques ». Nous avons constaté que la chaîne de Teams apporte des avantages, puisqu’elle permet de corriger l’ancien problème selon lequel seules certaines personnes sont au courant des approbations ou des exemptions dans la gestion des risques.

Recommandation nº 4

Tableau 5 : Avancement

Mise à jour de la direction	Évaluation du BVG
Partiellement achevée	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 en 2018 :

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 :

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

La direction des TI a examiné son budget actuel pour s'assurer qu'elle disposait du financement à consacrer à la maîtrise des risques priorisés. Le budget opérationnel de la sécurité et des risques de TI a été augmenté d'environ 80 % dans la période comprise entre 2018 et 2020.

On a créé le « Fonds de renouvellement des TI » en faisant appel à des dépenses en immobilisations pour financer une sélection de projets de technologie jugés prioritaires pour l'administration municipale, notamment les projets qui permettent aux STI de gérer efficacement et proactivement les risques de sécurité de l'administration municipale. Ce fonds est géré par le chef de l'information, qui travaille de concert avec la Direction générale des services des finances pour dresser chaque année la liste des projets, établir un plan de dépenses général et préparer un plan budgétaire pour répondre aux impératifs opérationnels correspondants.

La Direction de la sécurité technologique a aussi enrichi son effectif de trois postes, dont un responsable spécialisé pour la fonction de gestion des risques de sécurité.

On a créé, au sein de l'équipe de la direction des TI, le nouveau poste de directeur, Sécurité de l'information et Gestion des risques numériques, qui relève directement de la directrice générale de la Direction générale des services novateurs pour la clientèle. Le titulaire de ce poste doit s'assurer que la gestion des risques est à la fois intégrée et maximisée afin de prendre de meilleures décisions dans la gestion des risques au sein de l'administration municipale. Il doit également assurer l'amélioration continuelle du programme de gestion des risques pour la sécurité.

Recommandation nº 5

Tableau 6 : Avancement

Mise à jour de la direction	Évaluation du BVG
Achevée	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;
- inclut 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;
- comprend 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 en 2018 :

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 :

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

Cette évaluation se rapporte également à la recommandation 3.

On a créé dans Microsoft Teams un canal consacré à la GRST à l'intention des membres de l'organisme de gouvernance de la GRST; ce canal est désormais utilisé pour tenir les discussions sur les risques et pour enregistrer et consigner les approbations. La direction a fourni la preuve de cinq cas distincts dans lesquels on a discuté des risques sur la chaîne de Teams. Il s'agit entre autres d'un certain nombre d'exceptions se rapportant à la COVID-19 et de la connectivité à assurer pour le télétravail.

La direction a fait savoir qu'à son avis, « la chaîne de Teams est un moyen efficace et efficient d'avoir des échanges sur le mandat de la gouvernance de la GRST, surtout dans la foulée du scénario de télétravail forcé en réaction à la pandémie mondiale. Le

mandat approuvé fait état de cette plateforme de réunion ». La direction prévoit aussi de préciser que cette méthode de consultation est « la méthode privilégiée pour les évaluations types des risques ».

Nous avons constaté que la chaîne de Teams apporte des avantages, puisqu'elle permet de corriger l'ancien problème selon lequel seules certaines personnes sont au courant des approbations ou des exemptions dans la gestion des risques. Compte tenu de la crise sanitaire et du télétravail, nous sommes conscients des avantages de recourir à cette plateforme, à la condition de pouvoir archiver le contenu et de le conserver pour le consulter ultérieurement.

En outre, la direction devrait se demander s'il est avantageux de réunir une documentation plus rigoureuse sur les réunions mêmes consacrées à l'évaluation des risques, afin de consigner par écrit les décisions adoptées dans la gestion des risques et pour que l'information puisse être consultée ultérieurement.

Recommandation nº 6

Tableau 7 : Avancement

Mise à jour de la direction	Évaluation du BVG
Partiellement achevée	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 en 2018 :

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.

Mise à jour de la direction en 2020 :

Veuillez consulter la réponse apportée à la recommandation 1.

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 achevées.

Nous avons constaté que la version 2.0 consignée par écrit pour le Cadre de gestion des risques de TI (GRTI) décrit dans ses grandes lignes le modèle de gouvernance globale se rapportant à la gestion des risques et s'harmonise avec le Cadre de GRE de la Ville.

Le processus de validation annuelle des risques (VAR) est désormais en place, et nous avons examiné le « Rapport de validation annuelle des risques » de 2019, qui est daté du 24 janvier 2020. Ce rapport précise que « le processus de VAR constitue, pour l'ensemble de la Ville, le moyen de valider les risques évalués pour les technologies et leur sécurité et qui sont suivis par les Services de technologie de l'information lorsque leur cote indique qu'ils sont prioritaires ». Les résultats du processus de VAR ont permis de valider 23 risques et d'en ajouter un relativement à la Direction générale des transports.

On a créé dans Microsoft Teams un canal consacré à la GRST à l'intention des membres de l'organisme de gouvernance de la GRST; ce canal est désormais utilisé pour tenir les discussions sur les risques et pour enregistrer et consigner les approbations. La direction a fourni la preuve de cinq cas distincts dans lesquels on a discuté des risques sur la chaîne de Teams. Il s'agit entre autres d'un certain nombre d'exceptions se rapportant à la COVID-19 et de la connectivité à assurer pour le télétravail. La direction a fait savoir qu'elle préférait que les réunions se déroulent informellement et qu'il n'y ait pas de procès-verbal consigné par écrit pour ces réunions.

En outre, la direction prévoit aussi de préciser que cette méthode de consultation est « la méthode privilégiée pour les évaluations types des risques ». Nous avons constaté que la chaîne de Teams apporte des avantages, puisqu’elle permet de corriger l’ancien problème selon lequel seules certaines personnes sont au courant des approbations ou des exemptions dans la gestion des risques.

Recommandation nº 7

Tableau 8 : Avancement

Mise à jour de la direction	Évaluation du BVG
Achevée	Achevée

Recommandation de la vérification :

Que tous les services, avec le soutien des 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 des 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 de 2018 :

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.

Mise à jour de la direction de 2020 :

Veuillez consulter la réponse apportée à la recommandation 1.

En outre, les STI s'en remettent à ce qui suit pour recenser les risques dans le domaine des technologies et de leur sécurité :

1. la connaissance des normes de sécurité pour permettre au personnel de soutien des TI de signaler les risques;
2. les pratiques d'analyse de la vulnérabilité;
3. toutes les évaluations des menaces et des risques (EMR), qui sont désormais suivies dans le Registre des risques pour toutes les activités de suivi dans la maîtrise des risques et dans les exemptions;
4. le cycle de la durée utile des infrastructures d'après les documents de soutien des fournisseurs et les exigences de la Ville;
5. le cycle de la durée utile des applications d'après le modèle TIME (Tolérer, Investir, Migrer et Éliminer), qui est suivi dans la base de données de gestion des configuration (BDGC) des TI.

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 achevées.

Pour justifier la réalisation des autres évaluations des menaces et des risques (EMR) dans le cadre des changements apportés aux services existants, nous avons examiné un rapport sur les EMR pour l'équipement d'enregistrement des appels (version 2.0, en date du 12 août 2020). L'EMR s'est déroulée parce qu'il fallait mettre à niveau la technologie (« pour passer des enregistreurs d'appels Exacom G2 aux enregistreurs d'appels Exacom G3, soit la version la plus récente »). Le rapport donne un aperçu des résultats de l'évaluation de la sécurité de la migration d'Exacom et de l'infrastructure d'enregistrement des appels qui en découle.

La Ville a produit la version 2.0 à jour du document portant sur le Cadre de gestion des risques de TI le 13 décembre 2019. Le document à jour cadre désormais mieux avec la Politique de gestion des risques d'entreprise (PGRE) et fait état des rôles et des responsabilités de l'équipe de la Gestion des risques de sécurité des technologies (GRST), du chef de l'information, de l'équipe de dirigeants de la Direction générale, de la Direction de la sécurité des technologies (DST) et des Services de soutien aux activités.

On nous a fourni d'autres pièces justificatives relativement au tableur de suivi intitulé « Expérience 2020 de l'équipe de la sécurité ». Ce tableur fait état des certifications et de la formation (ainsi que de la participation aux conférences) de ceux qui font partie de l'équipe de la sécurité et qui peuvent être appelés à mener les évaluations des risques. On a constaté que les activités de formation et les certifications dans le domaine de la sécurité étaient nombreuses pour ceux qui occupent des postes clés et qui doivent prendre des décisions dans la gestion des risques pour la sécurité.

Comme nous l'avons noté dans les constatations précédentes, on a créé dans Microsoft Teams un canal consacré à la GRST à l'intention des membres de l'organisme de gouvernance de la GRST, et on s'en sert pour collaborer aux discussions sur les risques et pour consigner et enregistrer les approbations. La direction a fourni la preuve de cinq cas distincts dans lesquels on a discuté des risques sur la chaîne de Teams. Il s'agit entre autres d'un certain nombre d'exceptions se rapportant à la COVID-19 et de la connectivité à assurer pour le télétravail.

Recommandation nº 8

Tableau 9 : Avancement

Mise à jour de la direction	Évaluation du BVG
Achevée	Achevée

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 en 2018 :

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.

Mise à jour de la direction en août 2020 :

Le processus de validation annuelle des risques comprend une section consacrée à l'amélioration continuelle pour l'examen de la gouvernance mené par l'équipe de la gestion des risques de la sécurité technique. Dans le cadre de l'amélioration continuelle de l'ensemble du processus de gestion des risques, on examine chaque année les documents suivants :

- • le Cadre de GRTI;
- • le processus d'évaluation des risques des TI;
- • le Manuel du processus du Registre des risques de TI;
- • le processus d'exemption.

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 achevées.

Le BVG a procédé à l'examen de la version la plus récente (2.0) du document consacré au Cadre de gestion des risques de TI (GRTI), daté du 13 décembre 2019. Nous avons constaté que la section des révisions fait état des mises à jour apportées aux rôles et aux responsabilités dans la GRST, aux niveaux d'approbation et au modèle de cartographie des risques 5x5, ainsi qu'aux précisions portant sur la validation annuelle des risques de TI.

Le processus de validation annuelle des risques (VAR) est maintenant en place, et nous avons examiné le « Rapport sur la validation annuelle des risques » de 2019, daté du 24 janvier 2020. Ce rapport précise que « le processus de VAR constitue, pour l'ensemble de la Ville, le moyen de valider les risques évalués pour les technologies et leur sécurité et qui sont suivis par les Services de technologie de l'information lorsque leur cote indique qu'ils sont prioritaires ». Les résultats du processus de VAR ont permis de valider 23 risques et d'en ajouter un relativement à la Direction générale des transports. Ces résultats permettent de constater que toutes les évaluations des risques et tous les travaux de validation ont été menés par des membres compétents de l'équipe de la Direction de la sécurité technologique.

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	Aucune mesure n'est appliquée à l'heure actuelle; toutefois, la recommandation reste applicable.