3.6. Gestion des risques des technologies de l'information

Le 9 février 2021

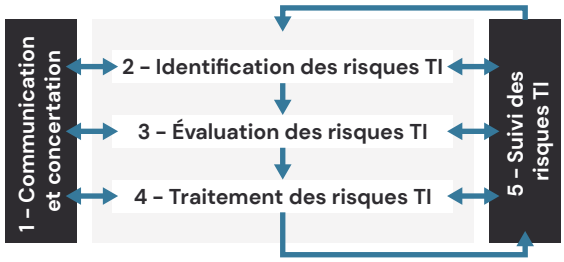
RAPPORT ANNUEL 2020
Bureau du vérificateur général
de la Ville de Montréal

Gestion des risques des technologies de l'information

Mise en contexte

La gestion des risques des technologies de l'information (TI) est un processus continu qui implique généralement les unités d'affaires (les propriétaires de la majorité des actifs informationnels) et le Service des technologies de l'information (STI).

Le diagramme suivant présente le cycle de vie de la gestion des risques TI :



Un risque TI est un événement, impliquant les TI, qui pourrait avoir un effet négatif sur la Ville de Montréal (la Ville), comme la perte ou le vol de données confidentielles, la non-disponibilité d'applications importantes, la non-conformité à des lois et règlements ou des pertes financières suite à une cyberattaque (p. ex. les rançongiciels).

Objectif de l'audit

Évaluer les processus, les outils et les contrôles mis en place par le STI afin de gérer efficacement les risques TI à la Ville et ainsi se protéger adéquatement face à divers événements pouvant affecter négativement les opérations ainsi que les services critiques de la Ville.

Résultats

Le STI a mis en place une équipe responsable d'appuyer la Ville dans sa gestion des risques technologiques. Cette équipe a réalisé des avancées notables à ce sujet. Cependant, nous concluons que la Ville ne dispose pas d'une gestion efficace des risques TI.

En effet, la gouvernance entourant la gestion des risques TI n'est pas suffisamment encadrée par une documentation complète, à jour, approuvée, diffusée auprès des parties prenantes et mise en application par ces dernières.

Le STI ne dispose pas des ressources humaines et technologiques nécessaires afin de répondre adéquatement à son offre de services en matière de gestion des risques TI.

Bien que le mécanisme de détection des risques technologiques soit documenté dans le processus de gestion des risques TI, il n'est pas mis en application.

Cette situation augmente la probabilité que la qualité de la gestion des risques TI soit très inégale d'une unité d'affaires à une autre ainsi que d'un intervenant à un autre et que les risques TI importants ne soient pas adéquatement détectés, pris en charge et suivis.

Principaux constats

Gouvernance et gestion des risques TI

- Des encadrements comme un modèle de gouvernance de sécurité de l'information, une politique, une directive et divers processus ont été développés par le STI en lien avec la gestion des risques TI. Néanmoins, certains de ces documents ne sont pas à jour, d'autres sont en cours de développement ou non approuvés ou non diffusés.
- Les activités de suivis et de reddition de comptes des risques TI, ainsi que de production d'indicateurs et de tableaux de bord des risques TI prévus dans le processus de gestion des risques TI ne sont pas mises en application.
- Le processus actuel de revue qualité du STI n'est pas documenté ni systématiquement réalisé par les parties prenantes.

Suffisance des ressources

- Le STI ne possède pas les ressources humaines et technologiques suffisantes afin de répondre adéquatement à son offre de services en matière de gestion des risques TI.

Détection des risques technologiques importants

- Le mécanisme de détection des risques technologiques est documenté dans le processus de gestion des risques TI. Cependant, étant donné que ce processus n'est pas finalisé, approuvé, ni diffusé auprès des parties prenantes, il n'est pas mis en application.

Analyse des risques TI

- Un processus ainsi que des outils et des gabarits ont été développés par le STI afin de faciliter la réalisation d'analyses des risques TI. Cependant, ils ne sont pas adéquatement complétés et la qualité globale des informations colligées varie d'une analyse à une autre.

Évaluation de la performance de la gestion des risques TI

- La performance de la gestion des risques n'est pas formellement évaluée sur une base régulière et communiquée auprès de la Direction générale de la Ville. Cette exigence se retrouve pourtant dans la *Politique de sécurité de l'information*.

En marge de ces résultats, nous avons formulé différentes recommandations aux unités d'affaires qui sont présentées dans les pages suivantes. Ces unités d'affaires ont eu l'opportunité de donner leur accord relativement aux recommandations.

Liste des sigles

GGRTI	Gouvernance et gestion des risques TI
STI	Service des technologies de l'information
TI	Technologies de l'information

Table des matières

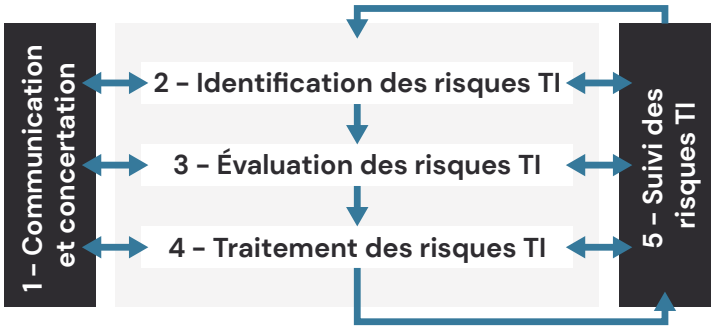
1. Contexte

La gestion des risques des technologies de l'information (TI) est un processus continu qui implique généralement les unités d'affaires (les propriétaires de la majorité des actifs informationnels) et le Service des technologies de l'information (STI).

Il est important que la Ville de Montréal (la Ville) gère efficacement ses risques TI considérant que :

- la Ville possède près de 300 applications informatiques[1] qui fonctionnent sous différents environnements technologiques en constante évolution;
- le développement, l'entretien et l'exploitation de ces systèmes requièrent la contribution de plus de 600 employés[2] du STI;
- le budget de fonctionnement de la Ville en technologies de l'information s'élèvera à plus de 100 M$[3] en 2021;
- tous les utilisateurs, autant les employés que les citoyens s'attendent à ce que ces systèmes soient performants, sécuritaires et disponibles.

Le diagramme suivant présente le cycle de vie de la gestion des risques TI :



Un risque TI est un événement, impliquant les TI, qui pourrait avoir un effet négatif sur la Ville, comme la perte ou le vol de données confidentielles, la non-disponibilité d'applications importantes, la non-conformité à des lois et règlements ou des pertes financières suite à une cyberattaque (p. ex. les rançongiciels).

[1] Selon une liste d'actifs informationnels obtenue du Service des technologies de l'information le 22 octobre 2020.

[2] Source : Plan triennal d'immobilisations 2019-2021.

[3] Budget de la Ville de Montréal – 2021.

Afin de se protéger contre l'avènement de ces effets négatifs, la Ville doit notamment réaliser régulièrement et selon une approche systématique des analyses de risques TI et ce, lors d'événements pouvant potentiellement déclencher ces risques TI, soient par exemple :

- des changements importants apportés à une application critique;
- le démarrage d'un projet TI comportant des données confidentielles;
- l'ajout ou la modification significative d'équipements technologiques;
- l'ajout d'un fournisseur TI important;
- un incident informatique majeur survenu à la Ville ou dans une autre organisation, mais qui pourrait survenir à la Ville;
- la découverte d'une vulnérabilité importante liée à un système critique de la Ville.

Suite à l'analyse de ces risques TI, un plan d'action doit être développé et réalisé par les unités d'affaires responsables, afin d'atténuer les risques les plus importants. Enfin, un suivi ainsi qu'une reddition de comptes formelle de l'avancement de ces plans d'action doivent être régulièrement effectués auprès des parties prenantes.

Voici les principaux types de risques TI pouvant être évalués lors de ces analyses :

- Divulgation d'informations confidentielles;
- Non-disponibilité de matériaux technologiques ou d'applications informatiques;
- Non-respect des lois et règlements de la Ville;
- Incapacité de poursuivre les activités d'affaires;
- Désastre naturel;
- Non-disponibilité ou défaillance d'un fournisseur;
- Manipulation de données;
- Performance dégradée.

Relevant du STI, la Division Gouvernance et gestion des risques TI (GGRTI) est composée de cinq conseillers en sécurité et elle a notamment pour mission d'appuyer les parties prenantes de la Ville dans la gestion de leurs risques TI.

Les services offerts par la Division GGRTI incluent entre autres la réalisation des livrables de sécurité suivants : un avis de sécurité, des analyses des exigences de sécurité, des analyses d'impacts, des analyses de risques TI et la coordination de tests d'intrusion informatique. À cela s'ajoute notamment le suivi des risques TI les plus importants ainsi qu'une reddition de comptes régulière de ces risques TI.

2. Objectif de l'audit et portée des travaux

En vertu des dispositions de la *Loi sur les cités et villes*, nous avons réalisé une mission d'audit portant sur la gestion des risques TI. Nous avons réalisé cette mission conformément à la *Norme canadienne de missions de certification* (NCMC) 3001, du Manuel de CPA Canada – Certification.

Le présent audit avait pour objectif d'évaluer les processus, les outils et les contrôles mis en place par le STI afin de gérer efficacement les risques TI à la Ville et ainsi se protéger adéquatement face à divers événements pouvant affecter négativement les opérations ainsi que les services critiques de la Ville.

La responsabilité du vérificateur général de la Ville consiste à fournir une conclusion sur les objectifs de l'audit. Pour ce faire, nous avons recueilli les éléments probants suffisants et appropriés pour fonder notre conclusion et pour obtenir un niveau d'assurance raisonnable. Notre évaluation est basée sur les critères que nous avons jugés valables dans les circonstances. Ces derniers sont exposés en annexe.

Le vérificateur général de la Ville applique la *Norme canadienne de contrôle qualité* (NCCQ 1), du Manuel de CPA Canada – Certification et, en conséquence, maintient un système de contrôle qualité exhaustif qui comprend des politiques et des procédures documentées en ce qui concerne la conformité aux règles de déontologie, aux normes professionnelles et aux exigences légales et réglementaires applicables. De plus, il se conforme aux règles sur l'indépendance et aux autres règles de déontologie du *Code de déontologie des comptables professionnels agréés*, lesquelles reposent sur les principes fondamentaux d'intégrité, de compétence professionnelle et de diligence, de confidentialité et de conduite professionnelle.

Notre audit a été réalisé de juillet à décembre 2020. Il a consisté à effectuer des entrevues auprès du personnel, à examiner divers documents et à réaliser les sondages que nous avons jugés appropriés en vue d'obtenir l'information probante nécessaire. Nous avons toutefois tenu compte d'informations qui nous ont été transmises jusqu'en février 2021.

À la fin de nos travaux, un projet de rapport d'audit a été présenté, aux fins de discussions, aux gestionnaires concernés au sein de chacune des unités d'affaires auditées ainsi qu'à chacune des unités d'affaires concernées, pour l'obtention de plans d'action et d'échéanciers pour leurs mises en œuvre.

3. Résultats de l'audit

3.1. Gouvernance et gestion des risques des technologies de l'information

3.1.1. Stratégie, politique et cadre de gestion

Les parties prenantes à une saine gestion des risques TI doivent avoir à leur disposition les encadrements stratégiques nécessaires afin de connaître notamment les orientations de la Ville en matière de gestion des risques TI et ainsi exercer les rôles et responsabilités attendus à cet effet.

Il n'existe pas un seul document qui présente directement la stratégie liée à la gestion des risques TI à la Ville. En effet, nous avons observé que cette stratégie est partiellement présentée dans les quatre documents suivants :

- Le modèle de gouvernance en sécurité de l'information;
- La *Politique de sécurité de l'information*;
- La Directive sur la gestion des risques TI;
- Le processus de gestion des risques TI.

Modèle de gouvernance en sécurité de l'information

Ce document présente notamment les responsabilités assignées aux unités d'affaires (1re ligne de défense), au chef de la sécurité de l'information et au STI (2e ligne de défense), ainsi qu'au contrôleur général (3e ligne de défense) et ce, en matière de sécurité de l'information et de gestion des risques TI.

Considérant que ce modèle assigne des responsabilités importantes à plusieurs unités de la Ville, il est important qu'il fasse l'objet d'une communication formelle par la Direction générale auprès de l'ensemble des parties prenantes, afin que ces dernières y adhèrent et priorisent la mise en application de ce modèle.

Nous avons constaté qu'une telle communication n'a pas été formellement réalisée. Cela amène le risque d'une faible adhésion des parties prenantes et d'une prise en charge incomplète des activités requises afin de gérer adéquatement les risques TI au sein de la Ville.

Politique de sécurité de l'information

Cette politique présente quelques encadrements en matière de gestion des risques TI à la Ville, notamment le :

- responsable d'un actif informationnel doit gérer les risques de cet actif;
- Comité de sécurité de l'information doit évaluer régulièrement la performance de la gestion des risques et en faire part auprès de la Direction générale.

Cependant, la dernière mise à niveau de cette politique date de 2006. Il est impératif de revoir rapidement le contenu de cette politique afin de s'assurer qu'elle répond bien à la réalité actuelle, notamment concernant les aspects liés à la gestion des risques TI.

Directive sur la gestion des risques des technologies de l'information

Cette directive a été présentée en janvier 2020 au Comité de sécurité de l'information. Elle a pour principal objectif de dicter une vision ainsi que des orientations communes en matière de gestion des risques TI à la Ville. Nous sommes d'avis qu'elle couvre adéquatement les principaux éléments attendus dans ce domaine.

En effet, on y présente les principes directeurs suivants :

- Associer la gestion des risques TI à la réalisation des objectifs stratégiques ou d'affaires de la Ville;
- Aligner la gestion des risques TI avec la gestion intégrée des risques de la Ville;
- Équilibrer les coûts et les avantages de la gestion des risques TI;
- Promouvoir une communication adéquate sur les risques TI;
- Établir un cadre organisationnel orienté vers une gestion efficace des risques TI;
- Intégrer le processus de gestion des risques TI aux activités quotidiennes de la Ville.

Cependant, cette directive n'est pas approuvée par la Direction générale, elle n'est pas diffusée auprès des parties prenantes, ni mise en application. En conséquence, cela amène le risque d'une non-uniformité des façons de faire en matière de gestion des risques TI.

Processus de gestion des risques des technologies de l'information

La documentation entourant le processus de gestion des risques TI n'est pas finalisée. Ainsi, elle n'est pas approuvée ni diffusée auprès des parties prenantes.

Cette situation amène le risque d'une non-uniformité des façons de faire en matière de gestion des risques TI, ainsi que d'un non-respect des rôles et responsabilités des parties prenantes lors de la réalisation d'activités liées à la gestion des risques TI.

Arrimage avec la gestion intégrée des risques

La gestion des risques TI est un sous-ensemble de la gestion intégrée des risques à la Ville. Les saines pratiques demandent à ce que la gestion des risques TI s'arrime aux encadrements développés et diffusés par le secteur responsable de la gestion intégrée des risques, et ce, afin de s'assurer d'une cohérence et d'une efficience dans les actions.

Comme le projet de la Ville, quant à la mise en place d'une gestion intégrée des risques, est en cours de réalisation, il serait possible que des principes directeurs en matière de gestion des risques TI (p. ex. l'appétit et la tolérance aux risques, les seuils d'impacts et de probabilité, les métriques des niveaux de risques) diffèrent de ceux qui seront plus tard définis par la gestion intégrée des risques.

Advenant de tels écarts, les évaluations de risques TI ne pourront pas être adéquatement comparées aux autres risques de la Ville (c.-à-d. un risque TI élevé pourrait être présenté comme étant moins important qu'un risque intégré de niveau « moyen »). Ainsi, la Ville ne serait pas en mesure de prioriser adéquatement ses actions en matière de gestion des risques TI.

3.1.1.A. Recommandation

Nous recommandons à la Direction générale de :

- s'assurer de la cohérence et de l'arrimage entre la gestion intégrée des risques et la gestion des risques des technologies de l'information, notamment en ce qui a trait à l'appétit et la tolérance aux risques, aux seuils d'impacts et de probabilité, ainsi qu'aux métriques des niveaux de risques;
- approuver la Directive de gestion des risques des technologies de l'information;
- s'assurer que la Directive est diffusée auprès des unités d'affaires et mise en application par ces dernières;
- communiquer formellement aux unités d'affaires son approbation et son engagement à l'égard du modèle de gouvernance de la sécurité de l'information, afin que ces dernières y adhèrent et priorisent la mise en application de ce modèle.

3.1.1.B. Recommandation

Nous recommandons au Service des technologies de l'information de :

- mettre à niveau et de diffuser la Politique de sécurité de l'information;
- finaliser la documentation entourant le processus de gestion des risques des technologies de l'information. S'assurer de sa diffusion et de l'adhésion des unités d'affaires.

3.1.2. Partage des rôles et responsabilités

Le partage des rôles et responsabilités des parties prenantes en matière de gestion des risques TI à la Ville est présenté essentiellement dans les quatre documents suivants :

- Le modèle de gouvernance en sécurité de l'information;
- La *Politique de sécurité de l'information*;
- La Directive de gestion des risques TI;
- Le processus de gestion des risques TI.

Modèle de gouvernance en sécurité de l'information

Ce modèle de gouvernance a été présenté au Comité de sécurité de l'information ainsi qu'à la Direction générale et adopté par ces derniers. On y retrouve notamment les responsabilités des unités d'affaires, du chef de la sécurité de l'information, du STI et du contrôleur général en matière de sécurité de l'information et de gestion des risques TI.

Politique de sécurité de l'information

Nous retrouvons dans cette politique certaines responsabilités assignées aux unités d'affaires ainsi qu'au comité de sécurité de l'information en matière de gestion des risques TI.

Directive sur la gestion des risques des technologies de l'information

Cette directive assigne des responsabilités en matière de gestion des risques TI à plusieurs intervenants, incluant :

- le Comité de gestion de la Direction générale;
- le Comité de sécurité de l'information;
- le contrôleur général;
- le chef de la sécurité de l'information;
- les unités d'affaires.

Processus de gestion des risques des technologies de l'information

Ce processus présente certaines responsabilités au contrôleur général, au STI, ainsi qu'aux unités d'affaires.

Nous constatons que l'ensemble des rôles et responsabilités ne sont pas formalisés. En effet, bien que plusieurs rôles et responsabilités soient définis adéquatement au sein de ces quatre documents, ceux-ci ne sont pas tous complétés, approuvés, ni diffusés auprès des parties prenantes (voir la section 3.1.1.).

Ainsi, certaines tâches risquent de ne pas être réalisées et d'autres pourraient avoir plusieurs responsables, ce qui peut engendrer un impact majeur sur la gouvernance et la qualité de la gestion des risques TI.

3.1.2.A. Recommandation

Nous recommandons au Service des technologies de l'information de :

- finaliser la documentation des rôles et responsabilités des parties prenantes du processus de gestion des risques des technologies de l'information suite à l'approbation de la directive afférente;
- s'assurer de la diffusion et de la bonne compréhension de ces rôles et responsabilités.

3.1.3. Procédures, guides et outils

Divers procédures, guides et outils liés à la gestion des risques TI ont été développés par le STI, afin de permettre aux parties prenantes la réalisation d'analyses des risques TI de qualité, notamment :

- un processus de gestion des risques TI;
- un gabarit pour encadrer les analyses de risques (incluant les niveaux de risques, d'impact et de probabilité, les types de risques à évaluer, les seuils de tolérance du risque);
- des gabarits liés à une demande d'analyse des risques, à l'acceptation, à la rédaction d'un rapport d'évaluation des risques, un autre gabarit advenant la dérogation d'un risque.

Processus de gestion des risques des technologies de l'information

Comme mentionné à la section 3.1.1. de ce rapport, ce processus n'est pas finalisé, approuvé, ni diffusé auprès des parties prenantes.

Ce processus prévoit que le STI réalise régulièrement un suivi des risques TI. En s'appuyant sur le registre des risques TI, le STI doit veiller à ce que les risques TI de la Ville soient sous contrôle et que les actions menées en la matière soient coordonnées et cohérentes. À cet effet, le STI doit mettre en œuvre des indicateurs afin de suivre les quatre états des risques qu'ils ont définis, soient :

- Non critique;
- En cours d'évaluation;
- En cours de traitement; ou
- Accepté par la Ville comme critique.

Ces indicateurs doivent être utilisés en vue d'améliorer, qualitativement ou quantitativement, le système de gestion des risques TI de la Ville. Ils doivent également alimenter différents tableaux de bord des risques TI.

Les indicateurs et tableaux de bord qui en résultent devraient être présentés régulièrement auprès des parties prenantes ainsi qu'à chaque rencontre du Comité de sécurité de l'information.

Suite à nos travaux, nous avons observé que ces activités de production d'indicateurs et de tableaux de bord, de suivis et de reddition de comptes des risques TI ne sont pas formellement et régulièrement réalisées.

Ainsi, il est possible que des risques TI importants ne fassent pas l'objet de l'attention requise auprès des parties prenantes et que la Ville soit exposée, à son insu, à des événements importants comme des pannes de systèmes critiques ou des cyberattaques qui menacent l'intégrité et la confidentialité de données détenues par la Ville.

Utilisation des gabarits lors des analyses de risques

Des gabarits ont été développés par le STI afin de faciliter la réalisation d'analyses des risques TI.

Nous avons observé que ces gabarits sont relativement complets. Cependant, ils ne sont pas finalisés et par conséquent ils n'ont pas été formellement approuvés ni diffusés auprès des parties prenantes. En conséquence, il est possible que la qualité des analyses des risques TI soit inégale et que les résultats ne décèlent pas des risques TI importants.

Afin d'évaluer dans quelle mesure ces gabarits sont adéquatement utilisés par les parties prenantes, et ce, lors des analyses de risques TI, nous avons sélectionné un échantillon de 6 projets TI sur les 50 ayant fait l'objet d'un accompagnement de la part d'un conseiller en sécurité de la Division GGRTI. Par la suite, nous avons analysé les documents produits suite à ces accompagnements et rencontré les conseillers en sécurité qui ont coordonné ces activités et participé à la production des livrables requis.

Globalement, nous observons pour notre échantillon de six projets :

- Trois projets comportaient des analyses des risques TI;
- Un projet comportait des impacts peu importants et ainsi ne nécessitait pas la réalisation d'une analyse des risques TI;
- Deux projets ont fait l'objet d'analyses d'impacts, cependant, les analyses des risques n'étaient pas encore réalisées.

Les trois analyses de risques TI évaluées ont été effectuées avec le gabarit prévu à cet effet et le résultat de celle-ci a été approuvé par les parties prenantes. Toutefois, nous avons noté que ces analyses étaient souvent incomplètes (c.-à-d. pas de détail des contrôles en place, de traitement du risque, pas de plan d'action, d'échéancier de réalisation du plan d'action).

De plus, certains autres gabarits sont rarement utilisés (p. ex. le gabarit de demande d'analyse des risques, le gabarit d'acceptation du risque).

En conséquence, le fait que la documentation des analyses de risques TI est incomplète et que certains gabarits ne sont pas utilisés amène le risque que la qualité des analyses de risques TI varie d'une analyse à une autre, pouvant mener à la matérialisation de risques importants mal évalués et non pris en charge. Ce qui demande la mise en place de revues qualité systématiques de ces analyses de risques TI.

Revue qualité

Nous avons observé qu'une revue qualité est parfois réalisée par une ressource du STI, suite à la production de divers livrables en lien à la gestion des risques TI.

Cependant, cette activité n'est pas encadrée par une documentation formelle, elle n'est pas réalisée systématiquement et elle ne couvre pas l'ensemble des activités et livrables du STI (c.-à-d. dans quelle mesure tous les gabarits attendus ont été adéquatement complétés, approuvés et diffusés).

Ainsi, il est possible que la revue qualité ne permette pas de détecter un non-respect de certains éléments attendus dans le processus de gestion des risques TI (c.-à-d. l'utilisation des gabarits attendus, l'obtention des approbations requises, la production des livrables demandés, le respect des étapes du processus). Cette situation pourrait mener à une analyse des risques TI incomplète ou qui ne répond pas aux attentes des parties prenantes.

3.1.3.A. Recommandation

Nous recommandons au Service des technologies de l'information de :

- mettre en place de manière récurrente un suivi et une reddition de comptes des risques des technologies de l'information auprès des parties prenantes;
- définir et mettre en place des indicateurs ainsi que des tableaux de bord liés aux risques des technologies de l'information. Les présenter régulièrement auprès des parties prenantes;
- approuver et diffuser les gabarits développés pour les analyses des risques des technologies de l'information;
- documenter et mettre en place un processus de revue qualité systématique des analyses de risques des technologies de l'information qui couvre l'ensemble des livrables et activités attendus.

3.2. Suffisance des ressources

Bien que la responsabilité de gérer les risques TI relève des unités d'affaires de la Ville, le STI est responsable de plusieurs activités liées à la gestion des risques TI, notamment de :

- développer et diffuser des encadrements liés à la gestion des risques TI;
- appuyer les unités d'affaires dans la gestion de leurs risques TI;
- produire divers livrables auprès des unités d'affaires liés à la gestion des risques TI (p. ex. l'avis de sécurité, l'analyse des exigences de sécurité, les analyses d'impacts, les analyses de risques TI, les évaluations de vulnérabilités, les tests de sécurité);
- alimenter et actualiser le registre des risques TI;
- faire le suivi des risques TI importants et en faire la reddition de comptes auprès des parties prenantes.

À cet égard, nous observons qu'avec les cinq conseillers en sécurité assignés à ces activités, le STI est uniquement en mesure de réaliser une partie de ces activités. En effet, comme constaté lors de nos travaux, voici les points importants :

- Des encadrements ne sont pas complétés, approuvés et diffusés auprès des parties prenantes;
- Seule une partie des projets TI font l'objet d'analyses de risques TI;
- Peu d'analyses de risques TI sont réalisées dans un contexte autre que celui d'un projet TI;
- La mise à jour du registre des risques TI est sporadique et non systématique;
- Les suivis systématiques des risques TI et leur reddition de comptes ne sont pas réalisés.

De plus, d'autres activités incluses dans l'offre de services du STI et en lien avec la gestion des risques TI ne sont actuellement pas réalisées, comme le développement et la diffusion systématique d'indicateurs de performance et de risques TI, le développement d'un programme de sensibilisation, de même que la gestion des tiers, lié à la gestion des risques TI.

Ainsi, nous constatons que le STI ne possède pas suffisamment de ressources humaines afin de réaliser adéquatement l'ensemble de ces activités importantes. Cette situation augmente la probabilité que des risques importants ne soient pas gérés adéquatement, qui pourrait occasionner une perte de disponibilité de systèmes critiques, le vol de données confidentielles ou l'avènement de cyberattaques importantes.

De plus, les principaux outils utilisés par le STI afin d'appuyer les unités d'affaires dans leur gestion des risques TI se limitent à des logiciels de bureautique et à un générateur de tableaux de bord. Ces outils ne permettent pas une gestion intégrée optimale des risques TI et forcent une approche manuelle dans la collecte, la mise à jour, le suivi et la reddition de comptes des risques TI.

Il existe pourtant sur le marché des outils technologiques intégrés facilitant :

- la compilation d'activités liées à la gestion de risques TI;
- le suivi systématique de ces risques TI;
- une reddition de comptes efficace des risques TI auprès des parties prenantes.

En conséquence, plusieurs saisies manuelles doivent être effectuées, ce qui amène entre autres des risques d'erreurs, d'omissions et de perte d'efficacité.

3.2.A. Recommandation

Nous recommandons à la Direction générale de s'assurer que le Service des technologies de l'information obtienne les ressources humaines et technologiques requises afin de répondre adéquatement à son actuelle offre de services en matière de gestion des risques des technologies de l'information.

3.3. Détection des risques technologiques importants

Afin que la Ville soit adéquatement protégée contre l'avènement d'événements significatifs comme le bris d'un système désuet menant à la non-disponibilité d'applications critiques ou à la perte de données suite à une cyberattaque informatique, il est nécessaire qu'un mécanisme efficace soit mis en place à la Ville, afin de détecter en temps opportun les risques TI importants.

Ce mécanisme de détection des risques TI est présenté dans le document : « Processus de gestion des risques TI ». Il consiste à assigner aux unités d'affaires, aux équipes de projets TI ainsi qu'à l'équipe liée à l'exploitation TI la responsabilité de déterminer, au regard des priorités de la Ville, les opérations nécessitant la réalisation d'une analyse des risques TI.

Lorsque l'une de ces parties prenantes décide qu'il est pertinent de réaliser une analyse des risques TI, celle-ci contactera la Division GGRTI du STI afin que cette dernière les appuie dans leur démarche.

De plus, afin de guider ces parties prenantes, ce processus présente quelques 12 événements pouvant mener à la réalisation d'analyses des risques TI, soient :

- l'intégration d'un nouveau produit ou service TI;
- l'évolution d'un système informatique;
- l'évolution des besoins des citoyens;

- les nouvelles exigences d'affaires;
- la modification de l'environnement opérationnel;
- la réorganisation du travail;
- le changement d'orientations stratégiques et/ou organisationnelles;
- la détection de menaces émergentes;
- l'identification de nouvelles vulnérabilités;
- l'évolution et/ou maintien de l'infrastructure TI;
- l'utilisation d'un nouvel outil/fonctionnalité TI;
- la mise à jour d'un correctif.

Nous sommes d'avis qu'afin que cette approche de détection des risques TI fonctionne efficacement, ces parties prenantes doivent :

- avoir reçu la documentation requise entourant ce processus;
- être pleinement sensibilisées face à leurs rôles et responsabilités en matière de gestion des risques TI;
- avoir démontré leur adhésion formelle face à ces responsabilités;
- avoir reçu une formation leur permettant de détecter efficacement leurs risques TI et d'appliquer adéquatement le processus de gestion des risques TI;
- communiquer régulièrement avec une ressource dédiée en gestion des risques TI du STI, et ce, afin de leur faire part de toute évolution en matière de risques TI (c.-à-d. les nouveaux risques, l'évolution des plans d'action visant à mitiger des risques importants, le changement de l'importance d'un risque).

Nous avons observé que ces cinq prérequis ne sont pas en place. En effet, comme mentionné à la section 3.1.1., la documentation entourant le processus de gestion des risques TI n'est pas finalisée. Ainsi, elle n'est pas approuvée, ni diffusée, ni mise en application par les parties prenantes. Il en résulte que les activités liées à la sensibilisation, l'adhésion, la formation et la communication régulière avec les parties prenantes n'ont également pas été complétées.

En conséquence, sans un processus efficace de détection, des risques TI importants ne feraient pas l'objet de l'attention requise et pourraient mener à l'avènement de situations critiques comme la non-disponibilité de systèmes, des cyberattaques informatiques qui peuvent occasionner le vol de données confidentielles ou la perte d'intégrité de données importantes.

3.3.A. Recommandation

Subordonnée à la recommandation 3.1.1.A. pour la partie concernant le processus de gestion des risques des technologies de l'information, nous recommandons au Service des technologies de l'information de:

- mettre en place un programme de formation et de sensibilisation des parties prenantes, notamment en regard à la détection des risques des technologies de l'information;
- prévoir un mécanisme efficace qui assurera le maintien d'une communication régulière entre le Service des technologies de l'information et les parties prenantes, et ce, afin de suivre l'évolution de leurs risques des technologies de l'information.

3.4. Analyse des risques technologiques

Le processus d'analyse des risques technologiques fait partie du processus de gestion des risques TI. Divers gabarits ont été produits par le STI afin de faciliter la réalisation de ces analyses par les parties prenantes.

Cependant, comme indiqué dans la section 3.1.1., le processus de gestion des risques TI n'est pas finalisé, ni approuvé, ni diffusé. Cette situation amène le risque d'une non-uniformité des façons de faire en matière d'analyse des risques TI.

De plus, dans la section 3.1.3., il est mentionné que ces gabarits n'ont pas été approuvés, ni diffusés formellement. Ce qui amène le risque que la qualité des analyses de risques TI varie d'une analyse à une autre, qui pourrait mener à la matérialisation de risques importants mal évalués et non pris en charge.

Afin de valider la qualité du processus d'analyse des risques TI, des tests d'efficacité ont été effectués sur un échantillon d'analyses des risques TI (voir la section 3.1.3.). Le résultat de ces tests démontre que la qualité de ces analyses est inégale, ce qui demande la mise en place d'une revue de qualité régulière de l'ensemble des étapes du processus de gestion des risques TI.

Aucune autre recommandation n'est requise, puisque nos constatations font déjà l'objet des recommandations 3.1.1.A, et 3.1.3.A.

3.5. Évaluation de la performance de la gestion des risques des technologies de l'information

La *Politique de sécurité de l'information* mentionne que la performance de la gestion des risques TI doit être régulièrement évaluée par le Comité de sécurité de l'information et les résultats de cette évaluation doivent être rapportés à la Direction générale.

L'évaluation de la performance permet de s'assurer que la gestion des risques TI répond adéquatement aux attentes de la Ville et qu'elle évolue régulièrement afin de s'adapter aux fréquents changements technologiques.

Nous avons observé que le Comité de sécurité de l'information ne réalise pas formellement et de façon régulière cette activité. Conséquemment, il n'est pas possible de s'assurer que la gestion des risques TI répond aux orientations stratégiques de la Ville.

3.5.A. Recommandation

Subordonnée à la mise en place des autres recommandations de ce rapport, nous recommandons au Service des technologies de l'information d'évaluer formellement et de façon régulière la performance de la gestion des risques des technologies de l'information et de présenter les résultats de cette évaluation à la Direction générale.

4. Conclusion

Le Service des technologies de l'information (STI) a mis en place une équipe responsable d'appuyer la Ville de Montréal (la Ville) dans sa gestion des risques technologiques. Cette équipe a réalisé des avancées notables à ce sujet. Cependant, nous concluons que la Ville ne dispose pas d'une gestion efficace des risques des technologies de l'information (TI).

En effet, selon nos travaux d'audit, la gouvernance entourant la gestion des risques TI n'est pas suffisamment encadrée par une documentation complète, à jour, approuvée, diffusée auprès des parties prenantes et mise en application par ces dernières. Sans une telle documentation, les parties prenantes à la gestion des risques TI ne disposent pas de toutes les informations requises afin de gérer efficacement et uniformément les risques TI dans leurs secteurs d'activité.

De plus, le mécanisme de détection des risques TI est documenté dans le processus de gestion des risques TI. Cependant, étant donné que ce processus n'est pas finalisé, approuvé, ni diffusé auprès des parties prenantes, il n'est pas mis en application. Ainsi, il est possible que des événements comportant des risques TI significatifs ne soient pas évalués et que cela génère des bris de services, des pannes de systèmes ou des pertes de données confidentielles.

Afin de répondre à son offre de services en matière de gestion des risques TI, le STI devrait s'assurer de disposer des ressources humaines et technologiques nécessaires. Nous observons qu'elles sont actuellement insuffisantes. Ainsi, certaines activités prévues dans son offre de services sont peu ou pas réalisées, ce qui expose la Ville à des risques supplémentaires.

Ce manque d'encadrement formel et de ressources humaines et technologiques augmente la probabilité que :

- la qualité de la gestion des risques TI soit très inégale d'une unité d'affaires à une autre et d'un intervenant à un autre;
- les risques TI importants ne soient pas adéquatement détectés, pris en charge et suivis.

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

1. Critère d'évaluation – Gouvernance et gestion des risques des technologies de l'information

Des encadrements comme un modèle de gouvernance de sécurité de l'information, une politique, une directive et divers processus ont été développés par le STI en lien avec la gestion des risques TI. Cependant, certains de ces documents doivent être mis à niveau, d'autres sont en cours de développement ou non approuvés ou non diffusés. Ainsi, plusieurs orientations et stratégies contenues dans ces encadrements ne sont pas actuellement mises en application par les parties prenantes. De plus, les rôles et responsabilités des parties prenantes à la gestion des risques TI ne sont pas tous adéquatement documentés à l'intérieur des encadrements.

Des procédures, des guides et des outils incluant notamment divers gabarits facilitant la gestion des risques TI ont été développés par le STI. En général, ces documents sont complets et à jour. Cependant, ces derniers ne sont pas tous approuvés et diffusés auprès des parties prenantes. Les activités de suivis et de reddition de comptes des risques TI, ainsi que de production d'indicateurs et de tableaux de bord des risques TI prévus dans le processus de gestion des risques TI ne sont pas mises en application. De plus, le processus actuel de revue qualité du STI n'est pas documenté ni systématiquement mis en application par les parties prenantes.

2. Critère d'évaluation – Suffisance des ressources

Le STI ne possède pas les ressources humaines et technologiques suffisantes afin de répondre adéquatement à son offre de services en matière de gestion des risques TI.

3. Critère d'évaluation – Détection des risques technologiques importants

Un processus de gestion des risques TI est en cours de développement. Ainsi, il n'est pas approuvé ni diffusé auprès des parties prenantes. Il présente notamment une approche visant à détecter et adresser des risques technologiques importants. Ce processus demande une participation active des unités d'affaires de la Ville. Toutefois, plusieurs prérequis devront être mis en place afin qu'il soit opérationnel et efficace.

4. Critère d'évaluation – Analyse des risques technologiques

Un processus ainsi que des outils et des gabarits ont été développés par le STI afin de faciliter la réalisation d'analyses des risques TI. Cependant, ils ne sont pas adéquatement complétés et la qualité globale des informations colligées varie d'une analyse à une autre.

5. Critère d'évaluation – Évaluation périodique de la performance de la gestion des risques des technologies de l'information et reddition de comptes auprès des parties prenantes

La performance de la gestion des risques n'est pas formellement évaluée sur une base régulière et communiquée auprès de la Direction générale de la Ville. Cette exigence se retrouve pourtant dans la *Politique de sécurité de l'information*.

5. Annexe

5.1. Objectif et critères d'évaluation

Objectif

Évaluer les processus, les outils et les contrôles mis en place par le Service des technologies de l'information afin de gérer efficacement les risques des technologies de l'information (TI) à la Ville de Montréal (la Ville) et ainsi se protéger adéquatement face à divers événements pouvant affecter négativement les opérations ainsi que les services critiques de la Ville.

Critères d'évaluation

Nous avons basé notre audit sur les critères d'évaluation suivants répartis en cinq volets :

1. Gouvernance et gestion des risques TI

1.1. Il existe une stratégie, des politiques et un cadre de gestion spécifique lié à la gestion des risques TI à la Ville. Ces documents sont complets, à jour, formellement approuvés et diffusés auprès des parties prenantes et mis en application par ces derniers.

1.2. Les rôles et responsabilités des parties prenantes à la gestion des risques TI à la Ville sont documentés, complets, à jour, formellement diffusés auprès des parties prenantes et mis en application par ces derniers.

1.3. Des procédures, des guides et des outils (incluant notamment une taxonomie des risques, son niveau de tolérance aux risques) ont été développés, afin de faciliter la gestion des risques TI. Ces outils sont complets, à jour, formellement diffusés auprès des parties prenantes et mis en application par ces derniers.

2. Suffisance des ressources

Des ressources suffisantes et adéquates sont présentent, afin de mettre en place une gestion des risques TI qui répond aux saines pratiques de l'industrie.

3. Détection des risques technologiques importants

Un processus est en place afin de détecter et adresser efficacement les risques technologiques importants. Ce processus inclut notamment la surveillance systématique des éléments suivants :

- Les risques émergents;
- Les événements de sécurité;
- Les risques liés aux nouveaux projets TI;
- Les changements technologiques importants.

4. Analyse des risques technologiques

Le processus d'analyse des risques TI inclut notamment :

- la collecte de données;
- l'implication formelle des parties prenantes;
- la détermination ainsi que la justification de l'impact d'affaires et de la probabilité;
- la description des contrôles;
- la détermination du risque résiduel;
- l'évaluation du risque résiduel par rapport à la tolérance au risque;
- le traitement du risque (c.-à-d. l'acceptation, le refus, la mitigation, le transfert);
- le cas échéant, le plan afin de mitiger adéquatement ce risque;
- présentation formelle des résultats de l'analyse aux parties prenantes et approbation par ces derniers.

5. Évaluation périodique de la performance de la gestion des risques TI et reddition de comptes auprès des parties prenantes

La performance de la gestion des risques est évaluée sur une base régulière et communiquée auprès de la Direction générale de la Ville.