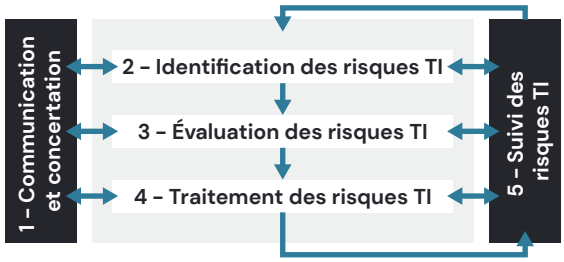
Gestion des risques des technologies de l'information

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.