



# 4.9.

## Gestion de l'informatique grise

Le 16 avril 2020

**Rapport annuel 2019**

Bureau du vérificateur général  
de la Ville de Montréal



# OBJECTIF

Déterminer si les mécanismes de contrôle, mis en place pour la gestion de l'informatique grise au sein de la Ville de Montréal (la Ville), permettent de réduire à un niveau acceptable les risques de perte de confidentialité, d'intégrité et de disponibilité des données.

L'informatique grise se définit par l'utilisation d'outils ou d'applications inconnue du Service des technologies de l'information.

# RÉSULTATS

Selon nos travaux, nous concluons que la Ville n'a pas mis en place de mécanismes de contrôle pour assurer une saine gestion de l'informatique grise. Sans gouvernance sur la gestion de l'informatique grise ni de processus de détection de l'informatique grise en production, la Ville n'a ainsi qu'une connaissance partielle de son utilisation par les unités d'affaires.

Ces constats jumelés au fait que la Ville affiche un retard dans la livraison de ses projets technologiques viennent augmenter la probabilité que les unités d'affaires se tournent vers des solutions de l'informatique grise.

Plusieurs améliorations sont requises au niveau de la gouvernance sur la gestion de l'informatique grise, de la stratégie de sensibilisation et de formation à l'informatique grise ainsi que du processus de détection.

Voici les principaux éléments nécessitant des améliorations :

- Il n'existe pas de gouvernance sur la gestion de l'informatique grise afin de définir l'informatique grise, les rôles et les responsabilités des parties prenantes et les mesures de sécurité.
- La stratégie de sensibilisation et de formation sur la Cybersécurité applicable à l'échelle de la Ville ne met pas suffisamment l'emphase sur les aspects afférents à l'informatique grise.
- Aucun processus de détection de l'informatique grise n'a été implanté.
- La gestion entourant les solutions de l'informatique grise, consistant à les évaluer et, selon les résultats de cette évaluation, à les approuver ou les rejeter, n'a pas été effectuée à ce jour.
- En l'absence de gouvernance encadrant la gestion de l'informatique grise, les saines pratiques attendues sur l'utilisation de l'informatique grise par les unités d'affaires ne sont pas en place.
- L'application goFinance vendue par l'arrondissement de Saint-Laurent, ne fait pas l'objet d'une entente de service pour quatre des neuf arrondissements utilisateurs tel que requis par la *Charte de la Ville de Montréal, métropole du Québec*.

*En marge de ces résultats, nous avons formulé différentes recommandations aux unités d'affaires.*

*Les détails de ces recommandations ainsi que notre conclusion sont décrits dans notre rapport d'audit présenté aux pages suivantes.*

*Soulignons que les unités d'affaires ont eu l'opportunité de donner leur accord et nous fournirons leurs commentaires ultérieurement.*



# TABLE DES MATIÈRES

<b>1. Contexte</b>	<b>473</b>
1.1. Définition de l'informatique grise	473
1.2. Principaux avantages de l'informatique grise	474
1.3. Principaux enjeux de l'informatique grise	475
<b>2. Objectif de l'audit et portée des travaux</b>	<b>476</b>
<b>3. Résultats de l'audit</b>	<b>478</b>
3.1. Gouvernance	478
3.2. Sensibilisation et formation	480
3.3. Détection de l'informatique grise	481
3.4. Gestion de l'informatique grise	482
3.5. Utilisation de l'informatique grise par les unités d'affaires	483
3.6. Entente de service pour la vente d'applications par un arrondissement	488
<b>4. Conclusion</b>	<b>492</b>
<b>5. Annexe</b>	<b>494</b>
5.1. Objectif et critères d'évaluation	494

# LISTE DES SIGLES

<b>CA</b>	conseil d'arrondissement
<b>PTI</b>	Programme triennal d'immobilisations
<b>STI</b>	Service des technologies de l'information
<b>TI</b>	technologies de l'information



## 1. CONTEXTE

À l'instar des autres grandes villes, organisations ou entreprises, la Ville de Montréal (la Ville) constate un accroissement du nombre d'applications, de logiciels, d'appareils ou de services sur son réseau, et ce, sans l'autorisation explicite du Service des technologies de l'information (STI). Cette pratique est désignée par le terme couramment utilisé d'informatique grise ou « *Shadow IT* »<sup>1</sup>.

### 1.1. Définition de l'informatique grise

Dans la Ville, la gestion des technologies de l'information (TI) est centralisée principalement sous le STI. L'informatique grise englobe tout élément qui compose un système d'information sans que le STI soit au courant. Ainsi, cela devient un élément en dehors de leur propriété ou de leur contrôle.

L'informatique grise consiste donc à utiliser, par exemple, des outils ou applications dont leur existence est inconnue du STI. Or, ce service ne peut pas protéger ce qu'il ignore. D'où l'importance pour celui-ci de connaître toutes les TI utilisées, incluant l'ensemble des applications.

Voici quelques exemples communs de l'informatique grise :

- Outils de collaboration;
- Outils de gestion des tâches;
- Bases de données spécialisées;
- Outil de gestion des ressources d'entreprise (ERP);
- Logiciel d'analyse financière;
- Solutions de transferts de fichiers ou d'échanges de données;
- Projets informatiques dans l'ombre de la Direction des TI.

---

<sup>1</sup> « *Shadow IT* » est un terme fréquemment utilisé pour désigner des systèmes d'information et de communication réalisés et mis en œuvre au sein d'organisations sans approbation de la direction des systèmes d'information.

Par le passé, l'informatique grise découlait du désir des employés à accéder à du matériel, des logiciels et des services Internet précis sans avoir à passer par les processus requis du STI. De nos jours, elle s'est développée davantage avec la gratuité de nombreux services en ligne auxquels les utilisateurs s'inscrivent sans tenir compte des dangers potentiels pour les systèmes informatiques de la Ville et la sécurité des données.

La consomérisation de l'informatique et les employés apportant des technologies grand public populaires dans l'organisation ont permis à ces derniers de déployer facilement des technologies sans que le STI soit averti.

L'utilisation de l'informatique grise est généralement symptomatique de la tendance des utilisateurs à croire, de leur point de vue, que la Direction des TI ne répond pas suffisamment à leurs besoins et donc qu'ils ne peuvent pas faire autrement. Leur compréhension des services rendus de la Direction des TI viendrait également influencer la pratique de l'informatique grise.

## **1.2. Principaux avantages de l'informatique grise**

Selon la perception du côté des utilisateurs, une des principales raisons pour laquelle les employés se tournent vers l'informatique grise est la volonté de travailler plus efficacement. En effet, pour être plus rapides, pour communiquer plus vite, ils utilisent des applications, des services, des fonctions de stockage et de partage d'informations sans passer par le secteur de l'informatique, car ils estiment que ce sera plus efficace et moins cher. Donc, en utilisant les technologies dont ils ont besoin sans permission, les employés considèrent qu'ils augmentent leur productivité.

Il est raisonnable de distinguer la bonne informatique grise de la mauvaise et ainsi de trouver un juste milieu pour permettre aux employés d'utiliser les solutions qui leur conviennent, tout en permettant à la Direction des TI de contrôler leur utilisation par des mesures de sécurité appropriées.



### 1.3. Principaux enjeux de l'informatique grise

Selon une étude de Gartner<sup>2</sup>, d'ici 2020, un tiers des attaques réussies rencontrées par les entreprises concernera leurs ressources *Shadow IT*.

Toujours selon Gartner :

*« [...] Business units deal with the reality of the enterprise and will engage with any tool that helps them do the job. Companies should find a way to track shadow IT, and create a culture of acceptance and protection versus detection and punishment. »*

Traduction libre :

*« [...] les unités d'affaires font face à la réalité de l'entreprise et s'engageront avec tout outil qui les aide à faire le travail. Les entreprises devraient trouver un moyen de surveiller le Shadow IT, et créer une culture d'acceptation et de protection par opposition à la détection et aux sanctions. »*

En 2016, Microsoft<sup>3</sup> a signalé que plus de 80 % des employés dans les organisations sondées ont avoué utiliser des solutions informatiques telles que des applications SaaS<sup>4</sup> dans l'infonuagique<sup>5</sup> sans l'accord de leur Direction des TI pour une utilisation en entreprise.

Les principaux enjeux de l'informatique grise sont les suivants :

- **Risque de sécurité** : Le principal risque de l'informatique grise est un risque de sécurité. Les logiciels et le matériel approuvés par les secteurs informatiques font l'objet d'importantes mesures de sécurité, ce qui n'est pas le cas des logiciels et matériels non approuvés. La Ville serait plus à risque de cyberattaques menées avec succès prenant comme cible leur informatique grise.
- **Fuite, perte, vol ou corruption de données** : Certaines applications telles que les services de partage ou de stockage de données comme Google Docs<sup>6</sup> ou DropBox<sup>7</sup> peuvent engendrer des fuites de données sensibles, stratégiques ou financières. Cela peut également créer une porte d'entrée dérobée et avoir pour conséquence la perte, le vol ou la corruption de données.

---

<sup>2</sup> Gartner, "Gartner's Top 10 Security Predictions 2016," June 15, 2016  
<https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/>

<sup>3</sup> Microsoft, "Microsoft Cloud App Security is generally available," 6 April 2016  
<https://www.microsoft.com/security/blog/2016/04/06/microsoft-cloud-app-security-is-generally-available/>.

<sup>4</sup> Logiciel en tant que service, ou Software as a Service, est un modèle de distribution de logiciels dans lequel un fournisseur tiers héberge les applications et les rend disponibles pour ses clients par l'intermédiaire d'internet.

<sup>5</sup> Mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services rendus par un fournisseur.

<sup>6</sup> Logiciel de traitement de texte basé sur internet de la suite bureautique de Google.

<sup>7</sup> Service d'entreposage et de partage de fichiers en ligne.

- **Non-conformité** : Ces applications représentent aussi un risque concernant la conformité aux lois et règlements tels que la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.
- **Capacité de la bande passante<sup>8</sup>** : Des outils et des applications utilisés sans le consentement de la Direction des TI peuvent affecter la bande passante disponible par une consommation accrue et s'avérer nuisibles pour les autres utilisateurs.
- **Coûts cachés** : Si ce n'est pas la Direction des TI qui effectue la phase de développement ou de configuration et de tests de l'outil, l'utilisateur le fera dans ses heures de travail durant lesquelles il ne réalisera pas les tâches pour lesquelles il est rémunéré.
- **Réputation** : la réputation de la Ville peut être grandement perturbée par des attaques ciblées fructueuses sur des composantes non gérées par la Direction des TI et accompagnée d'une perte de crédibilité et de confiance de ses citoyens.

Ces risques ne sont pas toujours connus des utilisateurs, même si les cas de cyberattaques et de vols de données sont de plus en plus présents dans les médias.

## 2. OBJECTIF DE L'AUDIT ET PORTÉE DES TRAVAUX

En vertu des dispositions de la *Loi sur les cités et villes* (LCV), nous avons réalisé une mission d'audit de performance portant sur la gestion de l'informatique grise. Nous avons réalisé cette mission conformément à la Norme canadienne de missions de certification (NCMC) 3001 du Manuel de CPA Canada – Certification ainsi qu'aux autres normes canadiennes de certification s'appliquant au secteur public émises par le Conseil des normes d'audit et de certification, soutenu par CPA Canada.

Le présent audit avait pour objectif de déterminer si les mécanismes de contrôle, mis en place pour la gestion de l'informatique grise au sein de la Ville, permettent de réduire à un niveau acceptable les risques de perte de confidentialité, d'intégrité et de disponibilité des données.

La responsabilité du vérificateur général de la Ville de Montréal consiste à fournir une conclusion sur l'objectif 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 à l'Annexe 5.

---

<sup>8</sup> Quantité d'informations pouvant être acheminées simultanément sur une voie de transmission.

Le vérificateur général de la Ville de Montréal 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.

L'objet de notre audit a porté uniquement sur les applications ou outils logiciels constituant de l'informatique grise. Plus précisément, ceux achetés ou disponibles gratuitement dans l'infonuagique. En résumé, ce sont les applications non gérées et non connues par le STI utilisées pour répondre à des besoins spécifiques.

Nous avons exclu de notre portée le matériel<sup>9</sup> pouvant répondre à la définition de l'informatique grise et les arrondissements n'étant pas gérés par le STI, car leurs achats informatiques ne constituent pas de l'informatique grise.

Afin de réaliser nos travaux d'audit, nous avons sélectionné les unités d'affaires suivantes :

- l'Arrondissement de Saint-Laurent;
- l'Arrondissement du Plateau-Mont-Royal;
- l'Arrondissement de Mercier–Hochelaga-Maisonneuve;
- l'Arrondissement de Côte-des-Neiges–Notre-Dame-de-Grâce;
- l'Arrondissement de Ville-Marie;
- l'Arrondissement de LaSalle;
- l'Arrondissement du Sud-Ouest;
- l'Arrondissement de Villeray–Saint Michel–Parc-Extension;
- le Service de l'environnement;
- le Service des ressources humaines;
- le Service de l'infrastructure du réseau routier;
- le STI.

Notre audit a été réalisé du 17 juillet 2019 au 16 janvier 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 avril 2020.

---

<sup>9</sup> Le matériel pourrait être par exemple une imprimante ou un serveur.

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. Par la suite, le rapport final a été transmis à la Direction générale ainsi qu'à chacune des unités d'affaires concernées, pour l'obtention de plans d'action et d'échéanciers pour la mise en œuvre des recommandations leur étant adressées. Une copie du rapport final a également été transmise au directeur général adjoint au Service aux citoyens, à la directrice générale adjointe de la Mobilité et attractivité, à la directrice générale adjointe de la Qualité de vie, à la directrice du Service de la concertation des arrondissements, aux directeurs et directrices des arrondissements non directement visés par nos travaux d'audit, afin qu'ils puissent mettre en œuvre les recommandations lorsque la situation le justifie.

## 3. RÉSULTATS DE L'AUDIT

### 3.1. Gouvernance

#### 3.1.A. Contexte et constatations

Une gouvernance sur la gestion de l'informatique grise devrait être formellement établie afin de circonscrire l'utilisation d'applications non approuvées et non gérées par le STI. Cette gouvernance consiste à définir un encadrement sur la gestion de l'informatique grise (i.e. sous la forme de directives et de standards) accessible à l'ensemble des employés de la Ville par l'intermédiaire de son site Intranet. Cet encadrement vise à définir ce qu'est l'informatique grise, les rôles et responsabilités, et à aborder une liste d'éléments pour prévenir, notamment, des comportements à risque, des fuites ou des vols d'informations.

Nous avons constaté l'absence d'encadrement sur la gestion de l'informatique grise. La définition de ce terme au sein même du STI varie d'une ressource à l'autre. La constitution de la Ville subdivisée en arrondissements, chacun dirigé par un conseil d'arrondissement (CA) distinct, vient accroître la complexité de l'application d'une gouvernance commune. Dans ce contexte, la gouvernance représente un enjeu majeur au sein de la Ville.

Nous avons constaté que la gestion de l'informatique grise ne fait partie d'aucun encadrement. L'élaboration d'un encadrement sur la gestion de l'informatique grise n'incombe pas juste au STI, car, en réalité, il ne gère pas en totalité les systèmes informatiques des unités d'affaires. La gouvernance doit émaner de la Direction générale de la Ville qui dispose de l'autorité appropriée pour en assurer l'adhésion de toutes les unités d'affaires et de tous les employés de la Ville, de son application et de son respect.

Le tableau 1 dresse le portrait des arrondissements quant à leur gestion TI.

Tableau 1 – **Portrait des arrondissements quant à leur gestion TI**

ARRONDISSEMENTS	GESTION TI
Ahuntsic-Cartierville	STI
Côte-des-Neiges–Notre-Dame-de-Grâce	STI
Le Plateau-Mont-Royal	STI
Le Sud-Ouest	STI
Mercier–Hochelaga-Maisonneuve	STI
Rivière-des-Prairies–Pointe-aux-Trembles	STI
Rosemont–La Petite-Patrie	STI
Ville-Marie	STI
Villeray–Saint-Michel–Parc-Extension	STI
Lachine	En cours de transfert au STI
LaSalle	En cours de transfert au STI
Pierrefonds-Roxboro	En cours de transfert au STI
Verdun	En cours de transfert au STI
Anjou	Arrondissement
L'Île-Bizard–Sainte-Geneviève	Arrondissement
Montréal-Nord	Arrondissement
Outremont	Arrondissement
Saint-Laurent	Arrondissement
Saint-Léonard	Arrondissement

L'absence d'encadrement fournissant les orientations formelles sur l'informatique grise au sein de la Ville ne permet pas au STI de promouvoir les saines pratiques entourant son utilisation. Cette situation pourrait engendrer l'utilisation d'applications non connues, non gérées et non approuvées par le STI de la Ville, telle que cela a été constaté dans certaines des unités d'affaires auditées.

Des rôles et des responsabilités non définis, non divulgués, et non connus des parties prenantes dans la gestion de l'informatique grise pourraient occasionner une hétérogénéité sur le droit d'utilisation de celle-ci, un accroissement de sa présence, des manquements et des non-conformités à son encadrement. Cela pourrait engendrer des failles de sécurité non détectées, des vols ou des pertes de données stratégiques et confidentielles (p. ex. des renseignements personnels).

## RECOMMANDATION

**3.1.B.** Nous recommandons à la Direction générale de définir une gouvernance de la gestion de l'informatique grise et de diffuser et maintenir à jour les encadrements afférents.

## RÉPONSE

**3.1.B.** Le rapport d'audit a été présenté à l'unité d'affaires visée entre le 25 février et le 15 avril 2020. Cette dernière est en accord avec la recommandation. Le Bureau du vérificateur général a demandé un plan d'action pour la mise en oeuvre de cette recommandation pour le 7 août 2020.

## 3.2. Sensibilisation et formation

### 3.2.A. Contexte et constatations

Une stratégie de sensibilisation et de formation à l'informatique grise permet de sensibiliser, de former et d'inculquer des comportements conformes aux orientations de la Ville à ce sujet. Elle contribue à faire prendre conscience aux employés des risques potentiels liés à l'utilisation de l'informatique grise, soit de vol, de divulgation ou de perte d'informations stratégiques ou confidentielles (p. ex. des renseignements personnels), de propagation de failles de sécurité et d'atteinte à la réputation. Elle vise donc à atténuer ces risques à un niveau acceptable pour la Ville.

Nous avons constaté que la Ville possède une stratégie de sensibilisation et de formation sur la Cybersécurité. Celle-ci permet de mieux comprendre la Cybersécurité, de reconnaître les menaces et de les prévenir par de bonnes habitudes. Le portail du STI de l'Intranet de la Ville comporte plusieurs capsules de formation à cet effet.

Cette stratégie s'intègre au projet « *Sensibilisation et formation des employés à la Cybersécurité – Sensibilisation des utilisateurs sur leur responsabilité de respecter les encadrements de sécurité et protéger les actifs informationnels* ». Cependant, la portée de cette stratégie n'englobe pas les aspects de l'informatique grise.

La stratégie de sensibilisation et de formation sur la Cybersécurité ne mettant pas suffisamment l'emphase sur l'utilisation de l'informatique grise et les responsabilités qui incombent à tous les employés pourrait occasionner des dysfonctionnements des applications critiques, des pannes de réseau informatique de la Ville découlant de cyberattaques menées avec succès ciblant leurs ressources de l'informatique grise et des pertes de confidentialité des données stratégiques et confidentielles (p. ex. des renseignements personnels).

## RECOMMANDATION

**3.2.B.** Nous recommandons au Service des technologies de l'information d'ajouter les aspects afférents à l'informatique grise à sa stratégie de sensibilisation et de formation sur la Cybersécurité applicable à l'échelle de la Ville de Montréal.

## RÉPONSE

**3.2.B.** *Le rapport d'audit a été présenté à l'unité d'affaires visée entre le 25 février et le 15 avril 2020. Cette dernière est en accord avec la recommandation. Le Bureau du vérificateur général a demandé un plan d'action pour la mise en oeuvre de cette recommandation pour le 7 août 2020.*

## 3.3. Détection de l'informatique grise

### 3.3.A. Contexte et constatations

La détection de l'informatique grise consiste à utiliser des procédés de découverte automatique ou manuelle de la présence de l'informatique grise. Cette détection vise à donner un portrait réel de l'ampleur de l'utilisation d'informatique grise et une assurance à la Ville que son environnement informatique est constitué d'applications et de logiciels approuvés par le STI. Ceux-ci devant faire l'objet d'importantes mesures de sécurité, ce qui n'est généralement pas le cas des applications et des logiciels de l'informatique grise.

Nous avons constaté que la Ville ne dispose pas d'un processus de détection de l'informatique grise. En effet, aucun outil de détection n'a été implanté sur le réseau de la Ville. Seule une démonstration de faisabilité sans intention d'achat est en cours sur un produit de détection de l'informatique grise, et ce, depuis plus d'un an. Nous avons obtenu, de l'équipe de la sécurité de l'information, un rapport préliminaire sur la situation de l'utilisation de l'informatique grise. Ce rapport se voulait une source de référence pour recenser les solutions de l'informatique grise détectées. Nous retrouvons par exemple des services d'entreposage dans le nuage ainsi que des services de conversion de document en ligne. Cependant, son niveau de détail insuffisant ne nous a pas fourni d'information sur le type de données transférées ni sur les utilisateurs de ces solutions. Par conséquent, le STI n'a qu'une connaissance partielle de son utilisation par les unités d'affaires.

L'absence d'un processus de détection de l'informatique grise pourrait occasionner sa prolifération et engendrer des failles de sécurité sans que le STI en ait connaissance. Il pourrait en résulter des vols ou des pertes de données stratégiques ou confidentielles (p. ex. des renseignements personnels).

## RECOMMANDATION

**3.3.B.** Nous recommandons au Service des technologies de l'information de se doter d'un processus de détection de l'informatique grise.

## RÉPONSE

**3.3.B.** *Le rapport d'audit a été présenté à l'unité d'affaires visée entre le 25 février et le 15 avril 2020. Cette dernière est en accord avec la recommandation. Le Bureau du vérificateur général a demandé un plan d'action pour la mise en oeuvre de cette recommandation pour le 7 août 2020.*

## 3.4. Gestion de l'informatique grise

### 3.4.A. Contexte et constatations

Une saine gestion de l'informatique grise consiste à évaluer si celle-ci représente la meilleure solution, en fonction des risques et ainsi déterminer si son utilisation est appropriée ou non. Après cette évaluation, une décision devrait être prise soit d'approuver ou de rejeter cette solution d'informatique grise avec les actions subséquentes correspondantes.

Nous avons constaté qu'aucune gestion de l'informatique grise n'a été effectuée à ce jour, à plus forte raison sans processus de détection.

De plus, le STI n'a pas défini de liste des applications permises pour permettre aux utilisateurs de les guider dans leur choix de solutions.

Sans gestion de l'informatique grise par le STI, cela pourrait occasionner la surabondance de solutions de l'informatique grise non autorisées par ce dernier. Ceci pourrait occasionner des failles de sécurité allant jusqu'à des vols ou pertes de données stratégiques ou confidentielles (p. ex. des renseignements personnels).

## RECOMMANDATION

**3.4.B.** Nous recommandons au Service des technologies de l'information de mettre en place un processus de gestion de l'informatique grise, et ce, subordonnée aux recommandations 3.1.B et 3.3.B.

## RÉPONSE

**3.4.B.** *Le rapport d'audit a été présenté à l'unité d'affaires visée entre le 25 février et le 15 avril 2020. Cette dernière est en accord avec la recommandation. Le Bureau du vérificateur général a demandé un plan d'action pour la mise en oeuvre de cette recommandation pour le 7 août 2020.*



## 3.5. Utilisation de l'informatique grise par les unités d'affaires

### 3.5.A. Contexte et constatations

L'utilisation de l'informatique grise au sein des organisations découle des besoins et demandes en services informatiques spécifiques pour les processus des unités d'affaires non livrés par le secteur des TI<sup>10</sup>. Cette réalité requiert l'implantation de saines pratiques de gestion de l'utilisation de l'informatique grise par les unités d'affaires pour éviter l'émergence de risques afférents à celle-ci.

En l'absence d'encadrements de la Ville, les saines pratiques recommandent aux unités d'affaires de maintenir un inventaire de l'informatique grise utilisée, de valider qu'aucun produit équivalent ne soit fourni par le STI, de réaliser une analyse de risques avant de choisir une solution d'informatique grise et, finalement, de définir les plans d'action pour atténuer les risques identifiés.

La mise en place de ces saines pratiques permet d'atténuer les risques, entre autres, de pertes d'homogénéité du parc informatique de la Ville et de contrôle des données stratégiques et confidentielles.

Nous avons sélectionné six unités d'affaires afin d'avoir une idée de l'ampleur de leur utilisation de l'informatique grise. Celles-ci sont :

- l'Arrondissement du Plateau-Mont-Royal;
- l'Arrondissement de Mercier-Hochelaga-Maisonneuve;
- l'Arrondissement de Côte-des-Neiges-Notre-Dame-de-Grâce;
- le Service de l'environnement;
- le Service des ressources humaines;
- le Service de l'infrastructure du réseau routier.

Lors de nos entrevues avec ces unités d'affaires, celles-ci nous ont mentionné qu'elles n'obtiennent pas tous les services demandés et attendus du STI, et que leurs besoins ainsi que leurs réalités ne sont pas nécessairement compris par celui-ci. Par exemple, l'utilisation par certaines d'entre elles de l'application goFinance (développée et vendue par l'arrondissement de Saint-Laurent) découle de besoins spécifiques non couverts (p. ex. de visualiser les données au moyen d'une interface Web, de forer l'information financière ainsi que de suivre les dépenses). L'application Qlik Sense, censée combler ces besoins est attendue depuis plus de deux ans.

---

<sup>10</sup> Référence : Atos, « *Shadow IT* : une augmentation de 20 % attendue en 2015 » Londres, le 30 mars 2015  
[https://atos.net/fr/2015/communiqués-de-presse/communiqués-généraux\\_2015\\_03\\_30/pr-2015\\_03\\_30\\_01](https://atos.net/fr/2015/communiqués-de-presse/communiqués-généraux_2015_03_30/pr-2015_03_30_01).

Parallèlement, dans le cadre d'une autre de nos missions d'audit sur la Gestion du bureau de projets du STI :

- Nous avons constaté que 99 projets sont prévus au Programme triennal d'immobilisations (PTI) 2020-2022 avec un budget qui varie entre 83 M\$ et 89 M\$ pour chacune de ces 3 années.
- Parmi les 41 projets en TI inscrits aux PTI de 2019-21 et de 2020-22 où un budget était requis, nous avons observé qu'environ 50 % de ceux-ci ont vu leurs échéanciers reportés de deux ans ou plus.
- Cette même statistique s'applique également aux 28 projets en TI inscrits au PTI priorisés en 2020 par le STI. En effet, 13 de ces 28 projets priorisés ont été reportés de deux ans ou plus dans le dernier PTI.

Ces reports dans la livraison des projets informatiques pourraient venir augmenter la probabilité que les unités d'affaires se tournent vers des solutions de l'informatique grise en provenance de l'infonuagique ou d'autres applications ne se trouvant pas sous le giron du STI.

La Ville n'ayant pas de processus de détection, il n'existe pas d'inventaire qui nous aurait permis de connaître quelles étaient les applications de type informatique grise utilisées par les unités d'affaires. De plus, lors des rencontres de démarrage de notre audit, les six unités d'affaires sélectionnées avaient porté à notre connaissance qu'elles ne savaient pas si leurs employés utilisaient des solutions de l'informatique grise, car cette notion leur était inconnue en raison de l'absence d'encadrement de la Ville à ce sujet. De ce fait, aucune des unités d'affaires rencontrées n'avait constitué d'inventaire relatif à l'informatique grise.

Après leur avoir expliqué en quoi consistait l'informatique grise, nous avons obtenu leurs listes d'applications de l'informatique grise produites manuellement et basées sur leur bonne foi. À partir de l'analyse de ces listes, nous avons constaté la présence d'applications en provenance de l'infonuagique, l'utilisation d'applications achetées ou développées à l'interne, et installées localement sur des systèmes informatiques de la Ville répondant à des besoins spécifiques.

Le tableau 2 dresse le portrait de l'informatique grise selon les informations obtenues dans chaque unité d'affaires rencontrée.

Tableau 2 – **Portrait de l’informatique grise selon les informations obtenues dans chaque unité d’affaires rencontrée**

<b>UNITÉS D’AFFAIRES (ARRONDISSEMENTS ET SERVICES)</b>	<b>APPLICATION DE L’INFORMATIQUE GRISE</b>	<b>APPLICATION INTERNET</b>	<b>APPLICATION À RISQUE<sup>11</sup></b>
Le Plateau-Mont-Royal	1	1	1
Côte-des-Neiges–Notre-Dame-de-Grâce	1	1	1
Mercier–Hochelaga-Maisonneuve	5	0	0
Service de l’environnement	0	N/A	N/A
Service des ressources humaines	38	10	1
Service des infrastructures du réseau routier	37	2	2
<b>TOTAUX</b>	<b>82</b>	<b>14</b>	<b>5</b>

<sup>11</sup> Applications Internet pouvant contenir des données stratégiques ou confidentielles.

Le tableau 3 indique les quatre applications Internet pouvant contenir des données stratégiques ou confidentielles, les risques associés ainsi que les arrondissements utilisateurs.

**Tableau 3 – Applications Internet pouvant contenir des données stratégiques ou confidentielles, les risques associés ainsi que les arrondissements utilisateurs**

APPLICATIONS INTERNET POUVANT CONTENIR DES DONNÉES STRATÉGIQUES OU CONFIDENTIELLES	TYPE DE RISQUES	ARRONDISSEMENTS UTILISATEURS
<p><b>Asana</b> <b>Outil de suivi de projet.</b></p> <p>Exemple de données : documents de travail, informations relatives aux grands livrables d'un projet, découpage des projets, tâches à accomplir.</p>	<ul style="list-style-type: none"> <li>• Risque de sécurité;</li> <li>• Fuite / vol ou corruption de données sur les livrables et les découpages d'un projet;</li> <li>• Réputation.</li> </ul>	<ul style="list-style-type: none"> <li>• Côte-des-Neiges–Notre-Dame-de-Grâce;</li> <li>• Service des ressources humaines.</li> </ul>
<p><b>DropBox</b> <b>Outil de dépôt de documents.</b></p> <p>Exemple de données : documents des consultants et entrepreneurs, vidéos, photos, plans.</p>	<ul style="list-style-type: none"> <li>• Risque de sécurité;</li> <li>• Fuite / vol ou corruption de données sur les documents de travail des consultants;</li> <li>• Réputation.</li> </ul>	<ul style="list-style-type: none"> <li>• Service des infrastructures du réseau routier.</li> </ul>
<p><b>Monday</b> <b>Outil de planification des ressources sur les projets.</b></p> <p>Exemple de données : avancement des projets, décomptes des ouvrages exécutés et des dépenses faites servant de base aux paiements à faire à l'entrepreneur.</p>	<ul style="list-style-type: none"> <li>• Risque de sécurité;</li> <li>• Fuite / vol ou corruption de données sur les décomptes des ouvrages exécutés et des dépenses faites;</li> <li>• Réputation.</li> </ul>	<ul style="list-style-type: none"> <li>• Service des infrastructures du réseau routier.</li> </ul>
<p><b>Trello</b> <b>Outil de gestion de projets pour simplifier la collaboration.</b></p> <p>Exemple de données : tableaux de gestion des tâches, données de géolocalisations (des adresses principalement), documents joints, photos, vidéos.</p>	<ul style="list-style-type: none"> <li>• Risque de sécurité;</li> <li>• Fuite / vol ou corruption de données sur les documents joints;</li> <li>• Réputation.</li> </ul>	<ul style="list-style-type: none"> <li>• Le Plateau-Mont-Royal.</li> </ul>

En l'absence d'encadrement sur la gestion de l'informatique grise ainsi que de stratégie de sensibilisation et de formation spécifique à celle-ci, les unités d'affaires ne disposent ni de la connaissance ni de la compétence pour mettre en place les saines pratiques de gestion attendues.

La mauvaise utilisation de l'informatique grise par les unités d'affaires pourrait engendrer des risques, entre autres, de pertes d'homogénéité du parc informatique de la Ville et de brèches de sécurité impactant la confidentialité et l'intégrité des données stratégiques et confidentielles.

### **RECOMMANDATION**

**3.5.B.** Nous recommandons aux arrondissements du Plateau-Mont-Royal, de Côte-des-Neiges–Notre-Dame-de-Grâce, de Mercier–Hochelaga Maisonneuve, au Service des ressources humaines et Service des infrastructures du réseau routier, dans l'attente de la mise en place des recommandations 3.1.B et 3.2.B, de :

- maintenir à jour leur inventaire relatif à l'informatique grise;
- valider qu'aucun produit équivalent ne soit fourni par le Service des technologies de l'information;
- réaliser une analyse de risques avant de choisir une solution de l'informatique grise;
- mettre en place des plans d'action pour atténuer les risques identifiés.

### **RÉPONSE**

**3.5.B.** *Le rapport d'audit a été présenté aux unités d'affaires visées entre le 25 février et le 15 avril 2020. Ces dernières sont en accord avec la recommandation. Le Bureau du vérificateur général a demandé un plan d'action, à chaque unité d'affaires, pour la mise en oeuvre de cette recommandation pour le 7 août 2020.*

## RECOMMANDATION

**3.5.C.** Nous recommandons au Service des technologies de l'information, dans l'attente de la mise en place des recommandations 3.1.B et 3.2.B, de sensibiliser et d'accompagner les unités d'affaires à l'effet de :

- maintenir à jour leur inventaire relatif à l'informatique grise;
- valider qu'aucun produit équivalent ne soit fourni par le Service des technologies de l'information;
- réaliser une analyse de risques avant de choisir une solution de l'informatique grise;
- mettre en place des plans d'action pour atténuer les risques identifiés.

## RÉPONSE

**3.5.C.** Le rapport d'audit a été présenté à l'unité d'affaires visée entre le 25 février et le 15 avril 2020. Cette dernière est en accord avec la recommandation. Le Bureau du vérificateur général a demandé un plan d'action pour la mise en oeuvre de cette recommandation pour le 7 août 2020.

## 3.6. Entente de service pour la vente d'applications par un arrondissement

### 3.6.A. Contexte et constatations

La *Charte de la Ville de Montréal, métropole du Québec* (Charte de la Ville) exige qu'une entente de service soit élaborée pour la vente d'applications par un arrondissement à un autre arrondissement. L'article 85.1 stipule que :

*« Un conseil d'arrondissement peut, aux conditions qu'il détermine, fournir au conseil d'un autre arrondissement un service relié à une compétence qu'il détient. La résolution offrant cette fourniture de service prend effet à compter de l'adoption d'une résolution acceptant cette offre. »*

Ainsi, la réalisation d'une entente de service entre deux arrondissements nécessite une résolution de chaque CA. L'adoption de ces résolutions fait foi de la conclusion de l'entente de service entre les deux arrondissements.

Un arrondissement ayant développé une application à l'interne pour ses besoins peut l'utiliser en raison de l'article 144 de la Charte de la Ville libellée comme suit :

*« Le conseil d'arrondissement est responsable de la gestion du budget d'arrondissement adopté par le conseil de la ville [...]. »*

Nous avons observé que l'application goFinance développée par l'arrondissement de Saint-Laurent a été vendue par celui-ci à neuf arrondissements de la Ville. Selon les informations obtenues des arrondissements, cette application répondrait à des besoins réels non desservis par le STI. En effet, l'application goFinance

permet la visualisation des données du système comptable SIMON au moyen d'une interface accessible par un fureteur Internet. Il aide à forer l'information financière concernant le budget de fonctionnement, les factures et les bons de commande émis aux fournisseurs et les dépenses de projets du PTI pour les cinq dernières années.

L'application goFinance est vendue par l'arrondissement de Saint-Laurent au prix de 50 000 \$ et des frais de 10 000 \$ sont facturés annuellement pour le support.

Le tableau 4 dresse la liste des dix arrondissements utilisateurs de l'application goFinance.

**Tableau 4 – Liste des dix arrondissements utilisateurs de l'application goFinance**

ARRONDISSEMENTS	SOUS GESTION STI
Côte-des-Neiges–Notre-Dame-de-Grâce	Oui
Le Plateau-Mont-Royal	Oui
Le Sud-Ouest	Oui
Mercier–Hochelaga-Maisonneuve	Oui
Ville-Marie	Oui
Villeray–Saint-Michel–Parc-Extension	Oui
LaSalle	En cours de transfert au STI
Pierrefonds-Roxboro	En cours
Saint-Laurent	Non
Saint-Léonard	Non

Nous considérons l'application goFinance comme de l'informatique grise, car huit des arrondissements sous le giron du STI l'utilisent sans l'en avoir informé au préalable.

Au sujet de la proposition d'entente de partenariat de services et des résolutions du CA requis à l'établissement d'une entente de service, le tableau 5 indique ce que nous avons constaté pour les neuf arrondissements acquéreurs de l'application goFinance.

Tableau 5 – **Arrondissements acquéreurs de l'application goFinance**

ARRONDISSEMENTS	PROPOSITION D'ENTENTE DE PARTENARIAT DE SERVICES (ARRONDISSEMENT DE SAINT-LAURENT)	RÉSOLUTION DU CONSEIL D'ARRONDISSEMENT VENDEUR (ARRONDISSEMENT DE SAINT-LAURENT)	RÉSOLUTION DU CONSEIL D'ARRONDISSEMENT ACQUÉREUR
Côte-des-Neiges–Notre-Dame-de-Grâce	Oui	Oui	Oui
LaSalle	Oui	Oui	Oui
Le Plateau-Mont-Royal	Non	Non	Non
Le Sud-Ouest	Non	Non	Non
Mercier–Hochelaga-Maisonneuve	Non	Non	Non
Ville-Marie	Oui	Oui	Oui
Villeray–Saint-Michel–Parc-Extension	Non	Non	Non
Pierrefonds-Roxboro	Oui	Oui	Oui
Saint-Léonard	Oui	Oui	Oui
<b>TOTAUX</b>	<b>5</b>	<b>5</b>	<b>5</b>

Ainsi, bien que neuf arrondissements aient acheté l'application goFinance, seulement cinq d'entre eux, soit Côte-des-Neiges–Notre-Dame-de-Grâce, LaSalle, Ville-Marie, Pierrefonds-Roxboro et Saint-Léonard, possèdent la proposition d'entente de partenariat de services de Saint-Laurent ainsi que les résolutions du CA des parties prenantes effectuées conformément à la Charte de la Ville.

L'absence de proposition d'entente de partenariat de services dûment complétée ainsi que d'adoption de résolutions des CA d'arrondissements est non conforme à la Charte de la Ville. De plus, l'absence de reddition de comptes sur cette situation ne permettrait pas aux élus, à la direction et aux unités d'affaires de la Ville d'en connaître son existence.



## RECOMMANDATION

**3.6.B.** Nous recommandons à l'arrondissement de Saint-Laurent dans le cadre de la vente de son application goFinance de :

- définir et soumettre une proposition d'entente de partenariat de services aux arrondissements acquéreurs;
- présenter et faire adopter une résolution à son conseil d'arrondissement.

## RÉPONSE

**3.6.B.** *Le rapport d'audit a été présenté à l'unité d'affaires visée entre le 25 février et le 15 avril 2020. Cette dernière est en accord avec la recommandation. Le Bureau du vérificateur général a demandé un plan d'action pour la mise en oeuvre de cette recommandation pour le 7 août 2020.*

## RECOMMANDATION

**3.6.C.** Nous recommandons aux arrondissements du Plateau-Mont-Royal, du Sud-Ouest, de Mercier-Hochelaga-Maisonneuve et de Villeray-Saint-Michel-Parc-Extension, dans le cadre de l'achat de l'application goFinance de :

- s'assurer d'obtenir la proposition d'entente de partenariat de services de l'arrondissement de Saint-Laurent;
- présenter et faire adopter une résolution à son conseil d'arrondissement.

## RÉPONSE

**3.6.C.** *Le rapport d'audit a été présenté aux unités d'affaires visées entre le 25 février et le 15 avril 2020. Ces dernières sont en accord avec la recommandation. Le Bureau du vérificateur général a demandé un plan d'action, à chaque unité d'affaires, pour la mise en oeuvre de cette recommandation pour le 7 août 2020.*

## 4. CONCLUSION

Selon nos travaux, nous concluons que la Ville de Montréal (la Ville) n'a pas mis en place les mécanismes de contrôles assurant une saine gestion de l'informatique grise. Sans gouvernance de la gestion de l'informatique grise ni de processus de détection de l'informatique grise en production, la Ville n'a ainsi qu'une connaissance partielle de son utilisation par les unités d'affaires.

Ces constats jumelés au retard que la Ville affiche dans la livraison de ses projets informatiques augmentent la probabilité que les unités d'affaires optent pour des solutions autres que celles offertes par le Service des technologies de l'information (STI), à savoir des solutions de l'informatique grise.

En effet, nous constatons que des améliorations significatives sont nécessaires, entre autres au niveau de l'encadrement sur la gestion de l'informatique grise, de la stratégie de sensibilisation et de formation à l'informatique grise ainsi que du processus de détection.

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

### **Critère d'évaluation – Gouvernance**

La Ville ne dispose pas d'encadrement couvrant les principales orientations stratégiques spécifiques à la gestion de l'informatique grise.

Le STI n'est donc pas en mesure de promouvoir les saines pratiques entourant l'utilisation de l'informatique grise, d'assurer une compréhension uniforme au sein des unités d'affaires ainsi que de développer et d'implanter les exigences requises pour la mise en place des contrôles minimaux.

Les rôles et responsabilités de ce processus n'ont pas été définis formellement.

### **Critère d'évaluation – Sensibilisation et formation**

La Ville possède une stratégie de sensibilisation et de formation sur la Cybersécurité. Néanmoins, la portée de cette stratégie ne met pas suffisamment l'emphase sur les aspects de l'informatique grise.

### **Critère d'évaluation – Détection de l'informatique grise**

La Ville ne dispose pas d'un processus de détection de l'informatique grise. Aucun produit de détection de l'informatique grise n'a été officiellement implanté sur le réseau de la Ville. Seule une démonstration est en cours sur la faisabilité sans intention d'achat d'un produit de détection. À ce stade-ci, le STI n'a aucun rapport détaillé sur l'utilisation de l'informatique grise à la Ville.

### **Critère d'évaluation – Gestion de l'informatique grise**

Aucune gestion de l'informatique grise n'est en place, consistant à évaluer les risques des solutions de l'informatique grise en production à la Ville et selon les résultats de cette évaluation à approuver ou à rejeter ces solutions.

### **Critère d'évaluation – Utilisation de l'informatique grise par les unités d'affaires**

Bien que cinq des six unités d'affaires de notre échantillon utilisent des applications de type informatique grise, les saines pratiques attendues sur l'utilisation de l'informatique grise par les unités d'affaires ne sont pas en place. Cela résulte de l'absence de gouvernance encadrant la gestion de l'informatique grise et de stratégie de sensibilisation et de formation couvrant ce sujet.

### **Critère d'évaluation – Entente de service pour la vente d'application par un arrondissement**

L'application goFinance, développée par l'arrondissement de Saint-Laurent et constituant de l'informatique grise, a été vendue à neuf arrondissements de la Ville. Seulement cinq d'entre eux respectent les exigences de la Charte de la Ville.

## 5. ANNEXE

### 5.1. Objectif et critères d'évaluation

#### Objectif

Déterminer si les mécanismes de contrôle, mis en place pour la gestion de l'informatique grise (« *Shadow IT* ») au sein de la Ville, permettent de réduire à un niveau acceptable les risques de perte de confidentialité, d'intégrité et de disponibilité des données.

#### Critères d'évaluation

##### Critère 1 : Gouvernance

Un encadrement sur l'informatique grise existe à la Ville afin de définir les exigences en matière de sécurité, l'appétit pour l'adoption et l'utilisation acceptable de l'informatique grise.

Les rôles et responsabilités des parties prenantes dans la gestion de l'informatique grise sont définis, divulgués et connus de celles-ci.

##### Critère 2 : Sensibilisation et formation

La sensibilisation à l'informatique grise de l'ensemble des employés est incorporée à la stratégie de formation et sensibilisation à l'échelle de la Ville.

Une formation sur l'informatique grise est donnée aux ressources spécialisées ciblées.

##### Critère 3 : Détection de l'informatique grise

Des processus sont en place au sein de la Ville pour découvrir l'utilisation de l'informatique grise rapidement. Ces processus incluent :

- les applications et logiciels non autorisés identifiés par des outils de découverte sont révisés;
- le trafic du réseau est surveillé pour détecter et réviser les solutions en TI non approuvées;
- les appels au service d'assistance technique et les incidents sont enregistrés pour détecter et analyser les systèmes qui ne sont pas dans l'inventaire des TI.

#### **Critère 4 : Gestion de l'informatique grise**

Les solutions de l'informatique grise sont évaluées en fonction des risques afin de déterminer si leur utilisation est appropriée pour la Ville.

Les solutions de l'informatique grise sont approuvées ou rejetées par une autorité compétente.

Les solutions de l'informatique grise sont classifiées en fonction des résultats de l'évaluation des risques et celles existantes sont examinées périodiquement dans le cadre du processus d'évaluation des risques.

Une action est prise suivant l'évaluation d'accepter et mitiger, ou rejeter la solution de l'informatique grise.

Ces actions consistent à :

- répertorier les informations détaillées des solutions de l'informatique grise dans l'inventaire des TI;
- définir le minimum des contrôles requis selon la classification de chaque solution de l'informatique grise;
- bloquer les solutions de l'informatique grise qui ont été rejetées et les remplacer en temps opportun par des applications entérinées.

#### **Critère 5 : Utilisation de l'informatique grise par les unités d'affaires**

- Les unités d'affaires maintiennent à jour leur inventaire relatif à l'informatique grise.
- Les unités d'affaires s'assurent qu'aucun produit équivalent n'est fourni par le STI.
- Les unités d'affaires réalisent une analyse de risques avant de choisir une solution de l'informatique grise et définissent les plans d'action pour mitiger les risques identifiés.

#### **Critère 6 : Entente de service pour la vente d'applications par un arrondissement**

Des ententes de services existent pour chacune des applications vendues par un arrondissement.

