Bureau du vérificateur général : Vérification de l’accès à distance aux technologies de l’information (TI), déposée devant le Comité de la vérification – Le 30 novembre 2017

Tables des matières

Vérification de l’accès à distance aux TI : en bref 1
L’objet de l’examen 1
La raison d’être de cette vérification 1
Les conclusions 1
Les constats 1
Vérification de l’accès à distance aux TI : résumé 5
Introduction 5
Renseignements généraux et contexte 5
Approche et méthodologie de la vérification 7
Portée 8
Résumé des principales constatations 8
Recommandations et réponses 19
Conclusion 21
Rapport de vérification détaillé 23
Vérification de l’accès à distance aux TI 23
Introduction 23
Renseignements généraux et contexte 23
Approche et méthodologie de la vérification 25
Portée 26
Approche et méthodologie de la vérification 26
Observations et recommandations de l’équipe de vérification 27
Annexe A : Objectifs et critères de la vérification 41

Remerciements

L’équipe responsable de la vérification, chapeautée par Orbis Risk Consulting sous la supervision de Sonia Brennan, vérificatrice générale adjointe, et la direction de Ken Hughes, vérificateur général, tient à remercier toutes les personnes qui ont contribué à ce projet, et plus particulièrement celles qui ont fourni des éclaircissements et des commentaires dans le cadre de la présente vérification.

Original signé par :

Le vérificateur général

Vérification de l’accès à distance aux TI : en bref

L’objet de l’examen

La vérification visait à évaluer dans quelle mesure la Ville d’Ottawa (la « Ville ») arrivait à détecter et à réduire efficacement les risques, notamment en matière de sécurité, associés à l’accès à distance à son réseau de technologies de l’information (TI). Elle avait aussi pour but de déterminer comment la Ville s’assurait d’offrir un réseau accessible et fonctionnel à distance, ainsi qu’un soutien rapide et efficace aux utilisateurs.

La raison d’être de cette vérification

La Ville s’appuie de plus en plus sur les technologies permettant aux employés et aux divers utilisateurs autorisés d’accéder à son réseau, même hors de ses murs. Si l’accès à distance accroît l’efficacité dans certaines situations d’affaires, il accroît en revanche le risque d’accès non autorisé, qui peut à son tour entraîner la perte ou la corruption de données, la divulgation de renseignements confidentiels ou privés et des interruptions de service.

Les conclusions

Il appert que les faiblesses et lacunes relatives aux pratiques et mesures de contrôle mises en œuvre pour prévenir l’accès non autorisé exposent les systèmes d’information de la Ville à divers risques importants, notamment la perte ou la corruption de données, la divulgation de renseignements confidentiels ou privés et des interruptions de service. Ces faiblesses touchent notamment les pratiques et contrôles techniques de sécurité desquels dépend la Ville pour détecter et prévenir les problèmes d’accès non autorisés et pour y réagir. Vu le rythme avec lequel les technologies évoluent et la dépendance accrue de la Ville à l’accès à distance, il est important de donner suite rapidement aux recommandations du présent rapport, ainsi qu’aux recommandations complémentaires formulées dans les vérifications antérieures en matière de TI.

Les constats

Même si la Ville a pris l’initiative d’améliorer certaines des mesures de contrôle pour l’accès à distance, la gestion des risques et la gouvernance, notamment la mise en œuvre planifiée d’une nouvelle norme sur la sécurité de l’information, nous avons relevé

des faiblesses et des lacunes qui requièrent une attention diligente. Nos constatations vont de l’absence d’une stratégie officielle sur l’accès à distance à certains problèmes techniques, décrits ci-après.

Stratégie relative à la technologie d’accès à distance – La Ville n’a pas de stratégie pour orienter et établir ses priorités, ses investissements et ses décisions en matière d’accès à distance. Par ailleurs, comme aucune autorité centrale n’est chargée de gérer les risques relatifs à l’accès à distance, il est d’autant plus probable que cette gestion manque de cohérence et ne soit pas optimale.

Recommandation – Le chef de l’information (CI) devrait s’assurer que la stratégie de la Ville en matière de TI permet d’offrir un accès à distance à toutes les directions générales et pour tous les services. Cette stratégie doit tenir compte de la manière dont les différentes directions générales assurent la connexion et la sécurité de l’accès à distance pour les services névralgiques. Par ailleurs, elle doit aborder les mesures à prendre dans la foulée des vérifications antérieures des TI, le cas échéant.

Recommandation – La Ville devrait veiller à l’adoption de la nouvelle norme relative à l’accès à distance, et voir à ce que toutes les directions générales de la Ville acceptent que le service en matière de sécurité soit centralisé. La norme devrait clairement définir la portée et les limites de l’environnement informatique de la Ville.

Recommandation – La Ville devrait prendre des mesures pour que l’examen et la mise à jour de ses politiques en matière de TI aient lieu au moins tous les deux (2) ans.

Architecture d’accès à distance – Nous avons constaté que la Ville n’a pas d’inventaire des technologies et modes d’accès à distance, et ceux-ci ne font pas non plus l’objet d’une cartographie détaillée, qui révélerait en outre la nature de l’information qui transige entre le réseau de la Ville et les points d’accès à distance. Sans de tels outils, il est très difficile de s’assurer que ces technologies et modes d’accès à distance sont appropriés et autorisés, et de confirmer que des mesures de sécurité efficaces sont en place.

Recommandation – La Ville devrait élaborer et tenir à jour un document ou un diagramme décrivant concrètement l’architecture du réseau des TI de la Ville, soit pour toutes les directions générales et pour tous les services. Les changements à l’architecture devraient être approuvés par le CI.

Recommandation – Comme un grand nombre d’intervenants, de directions générales et de services accèdent à distance au réseau de la Ville, cette dernière devrait créer un registre centralisé de toutes les solutions de connexion à distance utilisées au sein des

directions générales et de la Ville. Ce registre devrait définir le type d’accès à distance, indiquer comment il est isolé des réseaux des autres services de la Ville (ou connecté à ces derniers) et établir les facteurs à considérer ou les exigences en matière de sécurité. Les changements proposés au registre devraient être approuvés par le CI.

Lacunes de sécurité relatives à l’accès à distance – Bien que la vérification ait révélé la présence de différentes mesures de sécurité, l’accès à distance présentait certaines faiblesses et lacunes d’ordre technique. [redacted]

Recommandation – La Ville devrait prendre les mesures nécessaires pour mieux gérer les appareils mobiles, entre autres en instaurant des exigences et des mesures de contrôle techniques additionnelles en matière de sécurité pour l’accès à distance.

- [redacted]
- [redacted]

Surveillance et supervision – Il appert que la Ville a signé un contrat avec un nouveau fournisseur de services de sécurité gérés en juin 2016. [redacted] On constate aussi que la Ville n’envisageait toujours pas de faire un suivi et de mener des tests sur une base régulière, comme des évaluations de la vulnérabilité, des tests de pénétration et le rapprochement des comptes d’accès à distance. Ces mesures sont essentielles à la détection et à l’évaluation rapide des risques relatifs à l’accès à distance, qui sont en constante évolution.

Recommandation – La Ville devrait évaluer et améliorer la gestion et la surveillance de la sécurité de l’accès à distance, en prenant notamment les mesures suivantes :

- [redacted]
- Continuer d’améliorer les pratiques opérationnelles, entre autres la gestion et le rapprochement des comptes des fournisseurs et des employés.

Vérification de l’accès à distance aux TI : résumé

Introduction

La vérification de l’accès à distance aux TI figurait dans le Plan de vérification de 2016 du Bureau du vérificateur général (BVG), approuvé par le Conseil municipal en novembre 2015.

Renseignements généraux et contexte

Comme la plupart des organisations, la Ville d’Ottawa (la « Ville ») s’appuie de plus en plus sur la technologie pour atteindre une multitude d’objectifs stratégiques et opérationnels. L’une des nombreuses avancées technologiques des dernières années est la possibilité, pour les employés municipaux et autres utilisateurs autorisés, d’accéder au réseau des technologies de l’information (TI) à partir d’appareils autres que les postes de travail des bureaux municipaux. Cet accès a grandement amélioré l’efficacité du travail pour différents utilisateurs et dans de nombreuses situations opérationnelles. L’accès à distance n’est plus considéré comme une option, mais bien comme un outil essentiel du quotidien servant à répondre aux besoins en matière de TI des travailleurs mobiles (comme les paramédics et les agents des règlements), des fournisseurs (ceux qui en ont besoin pour voir à la maintenance et à la surveillance des applications et des systèmes) et des télétravailleurs, pour ne nommer que ceux-là.

Les besoins opérationnels et les avantages de l’accès à distance se multiplient, et les risques qui y sont associés s’accroissent proportionnellement. En effet, vu la prolifération de certaines technologies, comme les téléphones intelligents, et le foisonnement des options d’accès à distance, le risque d’accès non autorisé est de plus en plus grand. Les accès non autorisés pourraient entraîner différentes répercussions, comme la perte ou la corruption de données, la divulgation de renseignements confidentiels ou privés et des interruptions de service. Dans cet environnement, la Ville doit agir de façon proactive pour gérer les risques et les possibilités en matière de nouvelles technologies. Une telle approche comprend l’adoption de mesures visant à trouver un équilibre entre les avantages opérationnels et la nécessité d’assurer la sécurité des technologies et outils d’accès à distance actuels et futurs, au moyen de politiques, d’exigences, de lignes directrices et de pratiques.

La Ville a instauré un cadre stratégique et des exigences pour régir l’accès à distance, notamment la Politique sur l’utilisation responsable des ordinateurs, la Politique sur la sécurité des informations, la Politique sur les appareils technologiques et le Code de

conduite du personnel. Figurant parmi les politiques en matière de TI, la Politique sur l'accès à distance au réseau de la Ville, instaurée en 2006, vise tous les employés de la Ville qui nécessitent un accès à distance. Cette politique, dont la dernière mise à jour remonte à 2012, définit les responsabilités des utilisateurs, les processus d'autorisation et les mécanismes de sécurité permettant au personnel autorisé d'accéder à distance au réseau de la Ville. Elle décrit aussi l'offre de services[1] des Services de technologie de l'information (STI) de la Ville qui visent à soutenir l'accès à distance. Au moment de la vérification, les STI réalisaient un examen et une mise à jour exhaustifs du cadre stratégique en matière de TI, qui comprend la Politique sur l'accès à distance au réseau de la Ville. L'initiative a mené à la proposition d'un certain nombre de normes de sécurité technologique, notamment la nouvelle norme sur la sécurité de l'information pour les services d'accès à distance (*Information Security Standard - Remote Access Services* [ISS-RAS]). Comme il est expliqué plus loin, cette norme pallie certaines lacunes importantes du cadre stratégique actuel et clarifie les responsabilités et les pouvoirs du chef de l'information (CI). Ce dernier point est particulièrement important étant donné les solutions d'accès à distance personnalisées en usage dans différents secteurs comme OC Transpo, les Services d'eau, les Services de la circulation et la Bibliothèque publique d'Ottawa, qui ont recours à une équipe de TI autonome. Au moment de terminer la présente vérification, la mise en œuvre de cette nouvelle norme n'avait pas encore eu lieu.

Comme il est mentionné précédemment et décrit plus en détail dans le présent document, certains problèmes de gouvernance – notamment à propos des rôles, des responsabilités et des pouvoirs – ont mené à différentes observations lors de la vérification. Dans les dernières années, le Bureau du vérificateur général (BVG) a mené différentes vérifications des TI grâce auxquelles il a détecté différents problèmes de gouvernance, qui ont mené à un grand nombre des conclusions et recommandations du présent rapport. Les vérifications réalisées antérieurement sont la vérification de la gouvernance des TI (2014), la vérification de la gestion des risques liés aux TI (2015) et la vérification de la gestion des incidents liés à la sécurité des TI et des interventions en la matière (2015). Chacune de ces vérifications a permis de cibler des facteurs de risque liés à des technologies ou systèmes exclusifs gérés par des équipes de TI

[1] Les services suivants sont décrits dans la Politique sur l'accès à distance au réseau de la Ville : Web Mail, BlackBerry™, réseau privé virtuel (accès à partir d'un ordinateur portatif de la Ville) et les postes de travail à distance (accès à partir de l'ordinateur personnel d'un employé).

autonomes[2] plutôt que ceux gérés de façon centralisée par les STI. C'est pourquoi il est difficile pour la Ville de promouvoir des stratégies et des exigences relatives aux TI uniformes à l'échelle de l'organisation, y compris celles liées à la sécurité. De plus, ces vérifications ont permis de relever un manque de continuité systémique associé au poste de CI. Même si la vérification faisant l'objet du présent rapport ne se voulait pas un suivi des vérifications antérieures, mentionnons que ces deux problèmes sont toujours présents en 2017. Ils contribuent à accroître les risques relatifs à l'accès à distance et ont mené à bon nombre des constatations et des recommandations du présent rapport. Au cours de la vérification, le BVG a informé les STI des points communs entre les vérifications antérieures et les constatations et résultats de la présente vérification, et les a encouragés à donner suite avec diligence aux recommandations précédemment formulées. Conformément au protocole de vérification de la Ville, le BVG continue de prendre des mesures pour assurer le suivi actif de la réponse des STI aux constatations des vérifications antérieures.

Approche et méthodologie de la vérification

La vérification visait surtout à évaluer de façon indépendante la pertinence et l'efficacité des systèmes, pratiques et procédures, et de la gouvernance en place, afin de détecter et de réduire les risques associés à l'accès à distance au réseau de la Ville, notamment en matière de sécurité. Les éléments prioritaires sont les suivants :

- Recours à l'accès à distance;
- Rôles et responsabilités pour octroyer le droit d'accès;
- Architecture et technologie pour l'accès à distance;
- Fonctionnement et surveillance de l'accès à distance.

Des critères de vérification ont été établis en fonction des principaux guides en matière d'accès à distance aux TI, comme ceux publiés par le National Institute of Standards and Technology (NIST), notamment les éléments pertinents de son cadre de cybersécurité[3].

[2] Comme il est indiqué plus loin dans le présent rapport, l'existence d'équipes de TI autonomes ne signifie pas que les STI ne participent pas à la gestion des systèmes et technologies exclusifs, mais bien que leur participation ne se fait pas à titre d'autorité officielle.

[3] *Framework for Improving Critical Infrastructure Cybersecurity* (2014). Sur Internet :

https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Portée

La présente vérification porte sur les différents types d'accès à distance[4] offerts aux utilisateurs :

1. Les réseaux privés virtuels (VPN), par exemple :
    a. Protocole de sécurité IP (IPsec);
    b. Liens cryptés (couche de sockets sécurisés « protocole SSL »);
2. Connexions par contrôle à distance (par exemple Citrix et les solutions de bureau à distance);
3. Connectivité mobile (par exemple BlackBerry™, autres téléphones intelligents, tablettes);
4. Accès à distance sur le Web (par exemple Outlook Web Access).

L'examen visait aussi les mesures de contrôle au sein des STI et dans l'ensemble des secteurs d'activités et directions générales qui offrent un accès à distance, y compris les secteurs qui ont une équipe de TI autonome.

Il faut préciser que l'évaluation des réseaux privés virtuels (VPN) pour le travail à distance et l'accès par les membres du Conseil étaient exclus.

Résumé des principales constatations

Les constatations du présent rapport de vérification ont été regroupées selon les critères de vérification, soit dans quatre catégories :

- Stratégie;
- Inventaire et flux de données;
- Lacunes de sécurité;
- Surveillance et supervision.

Stratégie relative à la technologie pour l'accès à distance

Dans la vérification de la gouvernance des TI de 2014 du BVG, on notait que la Ville avait produit la *Feuille de route technologique,* qui cernait les priorités, les initiatives et les objectifs en matière de TI. Or, on relevait aussi un manque d'harmonisation entre les

[4] La vérification ne comprenait pas l'accès aux passerelles d'accès ou de communication qui ne peuvent se brancher directement au réseau de la Ville (p. ex., systèmes radio ou autres systèmes de communication).

investissements dans les TI de la Ville et ses priorités stratégiques et opérationnelles. La présente vérification révèle que la Ville n'a toujours pas trouvé de solution et n'a pas mis à jour sa *Feuille de route technologique 2013-2016.* Elle confirme en outre l'absence de plan pour élaborer une stratégie relative à la technologie d'accès à distance qui favoriserait l'harmonisation des priorités et de la prise de décision à l'échelle de la Ville, et clarifierait les responsabilités à l'égard des risques relatifs à l'accès à distance et la manière de les gérer. De plus, une telle stratégie permettrait de formuler une vision claire d'une approche efficace et globale qui devrait assurer un équilibre entre les besoins opérationnels et les exigences de sécurité, et coordonner la planification et la prise de décision dans des domaines émergents, comme les technologies mobiles.

Selon les constats établis lors de la vérification, l'absence de stratégie a contribué à certaines conclusions autour des thèmes suivants :

- Responsabilités à l'égard des risques relatifs à l'accès à distance qui menacent la sécurité du réseau et gestion de ces risques;
- Rôles, responsabilités et imputabilité;
- Gouvernance et prise de décision.

Même si la vérification a permis d'établir que les rôles, les responsabilités et l'imputabilité sur le plan opérationnel (p. ex., administration des comptes d'accès à distance, approbations et évaluation des risques) sont généralement clairs et font souvent l'objet de procédures et listes de vérification officielles, certains problèmes ont été relevés à l'échelon supérieur. Plus précisément, la responsabilité à l'égard des risques relatifs à l'accès à distance de la Ville, de même que les rôles, les responsabilités et l'imputabilité ne sont pas clairement établis au sein des différentes directions générales et de la Ville. Cette observation concorde avec les constatations de la vérification de la gestion des risques liés aux TI de 2015 du BVG, qui soulevait des problèmes similaires concernant l'autorité et les responsabilités du CI à l'égard des risques relatifs aux TI à l'échelle de la Ville.

La vérification indique que dans leurs sphères de responsabilité traditionnelles, les STI jouent un rôle efficace et approprié dans la surveillance[5], la supervision et la réduction des risques relatifs à l'accès à distance. Cependant, leur rôle ne s'étend pas

[5] Le suivi de la conformité est une responsabilité partagée de chaque direction générale (p. ex., suivi des comptes de personnes ne travaillant pas pour la Ville) et des STI (p. ex., suivi des comptes inactifs à l'échelle de la Ville).

officiellement au déploiement de l’accès à distance dans les directions générales où cet accès est géré par une équipe de TI autonome, ce qui, selon les vérifications antérieures du BVG, peut représenter un problème. Pour procéder à ces déploiements, la participation des STI à tous les volets de l’initiative – y compris dans la prise de décision névralgique – peut être soit minime, voire absente, soit très importante. Cette situation persistante limite la capacité des STI d’adopter une vision globale des technologies d’accès à distance de la Ville en vue de soutenir une planification économique et opérationnelle stratégique et efficace, ainsi qu’une bonne gestion des risques. Sans une autorité centrale porteuse d’une vision globale des technologies d’accès à distance, la gestion uniforme des risques en cette matière à l’échelle de l’organisation devient beaucoup plus difficile, ce qui menace la sécurité du réseau et risque d’entraîner le dédoublement des services.

Si la vérification a permis de relever des problèmes associés à l’absence d’une stratégie relative à la technologie d’accès à distance à l’échelle de la Ville pour orienter efficacement sa vision, elle a aussi permis de noter l’existence d’un certain nombre d’initiatives pour aider à les résoudre. Comme il est indiqué à la section *Renseignements généraux et contexte,* les STI effectuent actuellement un examen et une mise à jour exhaustifs du cadre stratégique en matière de TI de la Ville, qui comprendront le remplacement de la Politique sur l’accès à distance au réseau de la Ville actuelle, jugée désuète et largement inefficace. La nouvelle norme sur la sécurité de l’information pour les services d’accès à distance semble offrir une bonne couverture technique pour satisfaire aux exigences de l’accès à distance – notamment en matière de suivi, de tests et d’application de correctifs – et formule des attentes claires pour les utilisateurs finaux relativement à l’utilisation appropriée. De plus, la version provisoire de la norme indique clairement qu’elle s’applique à tous les services qui offrent une connexion à distance aux environnements informatiques de la Ville, notamment ceux gérés par des équipes de TI autonomes ou des tiers. Par ailleurs, elle clarifie l’obligation de faire approuver par le CI toute exemption aux obligations inhérentes à la norme. Voilà des éléments importants qui aideront à résoudre les problèmes soulevés dans la présente vérification et les vérifications antérieures[6]. L’approbation et la mise en œuvre de la nouvelle norme (en version provisoire depuis 2016) constitueront des étapes clés pour corriger les lacunes actuelles en matière de contrôle et d’uniformité de l’accès à distance à l’échelle de la Ville.

[6] Comme il est indiqué précédemment, la présente vérification ne se voulait pas un suivi des vérifications des TI antérieures du BVG.

Architecture pour l’accès à distance – Inventaire et flux de données

Vu l’importance accrue de l’accès à distance pour soutenir les activités opérationnelles, y compris certaines fonctions essentielles, les vérificateurs s’attendaient à trouver une architecture organisationnelle d’accès à distance consigné pour donner une vision d’ensemble de tous les types de connexion à distance offerts par la Ville. Un tel document donnerait des renseignements sur 1) l’interface des appareils d’accès à distance de toutes les directions générales de la Ville; 2) les technologies d’accès à distance en place, notamment celles relatives au SCADA ou aux applications exclusives avec connexion à distance; et 3) les flux de données associés (c.-à-d. la nature – comme le volume ou le caractère délicat – de l’information qui circule entre le réseau de la Ville et les appareils connectés à distance).

Or, la vérification a révélé que la Ville n’a consigné ni son architecture, ni l’inventaire exhaustif de ses technologies, connexions et flux de données relatifs à l’accès à distance, y compris dans les cas de déploiements par des directions générales auxquels les STI ne participent pas. Malgré l’absence d’une architecture organisationnelle, on peut trouver des documents sur l’architecture de certains services d’accès à distance de la Ville (infrastructure VPN ou BlackBerry™, connexion pour bureau à distance, etc.) ainsi qu’un inventaire des ordinateurs portatifs et téléphones intelligents appartenant à la Ville. De plus, l’équipe de vérification sait que les STI ont récemment conçu des plans et assigné certaines responsabilités en vue de créer un répertoire central des risques et des technologies relatives à l’accès à distance. Cependant, au moment de la vérification, l’absence d’un inventaire organisationnel exhaustif entraînait certaines répercussions pour la Ville, notamment l’incapacité à élaborer une planification stratégique efficace et à en tirer profit.

Sans planification stratégique, les investissements technologiques, les services et les procédures en matière d’accès à distance risquent d’être moins bien coordonnés et d’entraîner des dépenses inutiles ou inopérantes, ou la mise en place de mesures de sécurité inefficaces. Sur le plan opérationnel, cette lacune augmente la probabilité de différents problèmes : atteintes à la sécurité ou violation de règlements (p. ex. sur la vie privée) en raison de connexions à distance non conformes, retards dans la détection de ces atteintes ou violations, et utilisation de plateformes d’accès à distance non autorisées. Finalement, bien que la nouvelle norme sur la sécurité de l’information pour les services d’accès à distance (ISS-RAS) s’applique aux technologies de l’information qui soutiennent les connexions à l’environnement informatique de la Ville, cet

environnement doit être clairement défini pour limiter les divergences d’interprétation par les groupes qui composent la Ville.

Lacunes relatives à la sécurité de l’accès à distance aux TI

Bien qu’il soit essentiel sur le plan opérationnel d’offrir une connexion à distance fiable et hautement disponible dans l’environnement actuel, cette connexion pose certains risques quant à la sécurité des TI, par exemple en matière de confidentialité, d’intégrité et de disponibilité. Pour réduire et gérer ces risques, il faut que les pratiques et mesures de contrôle en matière de sécurité de la Ville permettent de prévenir et de détecter les incidents relatifs à l’accès à distance non autorisé au moyen des différents outils (VPN, bureau à distance, téléphones intelligents, etc.), puis d’y réagir. Il faudrait aussi qu’elles prennent en compte les exigences opérationnelles de la Ville et la nécessité des mesures de sécurité adéquates. Dans son examen des mesures de sécurité, les vérificateurs ont tenu compte des contextes ci-dessous.

- Points terminaux (c.-à-d. ordinateurs portatifs ou téléphones intelligents utilisés pour accéder au réseau de la Ville) – les appareils doivent être configurés et protégés de façon à empêcher l’accès non autorisé et toute autre activité posant un risque. Pour être sécuritaire, un point terminal doit être crypté, demander un mot de passe sécuritaire, assurer une protection contre les maliciels et être géré de façon centralisée avec une configuration verrouillée.
- Architecture du réseau – la Ville doit prévenir l’accès à distance non autorisé au réseau de la Ville. La conception du réseau et l’architecture doivent permettre aux directions générales dont l’infrastructure est essentielle de s’isoler de l’accès à distance par le réseau de la Ville.
- Services de soutien – le soutien aux utilisateurs de l’accès à distance devrait être très disponible (p. ex., après les heures normales de bureau), être soumis à des mesures de sécurité appropriées (p. ex., validation de l’identité de l’utilisateur avant la prestation du service) et respecter les normes.
- Surveillance opérationnelle et détection d’incidents – la surveillance des activités et du trafic relatifs à l’accès à distance devrait permettre de relever les anomalies, les alertes et les problèmes potentiels de sécurité, et, le cas échéant, de procéder à l’intensification de l’intervention. Les mesures de contrôle examinées par les vérificateurs comprennent celles imparties par la Ville à un fournisseur de services de sécurité gérés.

Dans le cadre de la vérification, l’équipe a examiné les mesures de sécurité mentionnées précédemment par une série de tests techniques : utilisation d’un

ordinateur portatif et d’un téléphone intelligent BlackBerry™ de la Ville pour se connecter à distance au réseau, et utilisation d’appareils n’appartenant pas à la Ville pour tester l’accès non autorisé au réseau et aux fonctionnalités de la Ville.

Les tests réalisés avec des appareils fournis par la Ville ont permis de constater qu’un certain nombre de mesures de sécurité efficaces sont en place et de confirmer la résilience des systèmes d’accès à distance et leur capacité à offrir une grande disponibilité. Les vérificateurs ont noté que l’architecture par défaut permet d’isoler les infrastructures essentielles du réseau général de la Ville. Concernant les mesures de sécurité précises, l’ordinateur portatif fourni par la Ville était beaucoup plus sécuritaire que le téléphone intelligent. L’ordinateur portatif offrait un contrôle efficace pour prévenir le contournement des restrictions (p. ex., mots de passe) ou le rehaussement non autorisé du niveau d’accès d’un utilisateur. De plus, l’ordinateur portatif était configuré avec un logiciel de sécurité à jour, son disque dur était entièrement crypté et il ne permettait pas l’exportation non autorisée d’un logiciel VPN sur un ordinateur portatif n’appartenant pas à la Ville.

L’équipe de vérification a réussi à obtenir d’autres résultats positifs à la suite de ses tests. Elle a notamment constaté que l’architecture du réseau d’accès à distance semblait peu vulnérable aux tentatives d’accès non autorisé. De même, les utilisateurs autorisés se voyaient imposer certaines restrictions relativement à l’accès et aux fonctionnalités lorsqu’ils se connectaient à distance à partir d’appareils n’appartenant pas à la Ville. De plus, les tests ont permis de conclure que la Ville avait mis en place des procédures opérationnelles de gestion de l’accès à distance appropriées pour l’utilisateur final et pour la bonne administration des comptes.

Cependant, les tests ont aussi révélé des problèmes en raison de certaines lacunes et faiblesses relatives à l’environnement de sécurité pour l’accès à distance. Celles-ci pourraient compromettre la capacité de la Ville à prévenir et à détecter les incidents, dont l’accès non autorisé, et à y réagir. Plus précisément, la vérification a permis de relever les problèmes techniques suivants en matière de sécurité de l’accès à distance :

- Les appareils mobiles fournis par la Ville ne sont pas suffisamment sécuritaires;
- [redacted]
- [redacted]

- La surveillance en matière de sécurité n’a pas été optimisée pour cibler les scénarios d’atteinte à la sécurité lors d’une connexion à distance et y réagir.

Ces problèmes sont décrits plus en détail ci-dessous.

Lors de la vérification, les tests réalisés avec un téléphone intelligent de la Ville[7] ont révélé que l’appareil mobile était configuré avec le plus récent système d’exploitation de BlackBerry™ et différentes mesures de sécurité, notamment la technologie BlackBerry Balance, servant à séparer les espaces professionnel et personnel. Par ailleurs, le système de gestion des appareils de la Ville envoie une alerte par courriel aux utilisateurs dès la détection d’activités anormales[8]. Cependant, l’appareil n’était pas suffisamment sécuritaire pour pallier les faiblesses et lacunes relevées.

- [redacted]
- [redacted]
- [redacted]

[redacted]

[7] La Ville est en voie de remplacer ses appareils BlackBerry™, y compris celui utilisé pour les tests lors de la vérification. Cependant, ce changement n’aura aucune incidence sur les constatations formulées, qui demeureront valides.

[8] Dans ce cas, l’alerte indiquait que l’appareil n’était plus conforme aux politiques et paramètres de sécurité visant à protéger les renseignements et le réseau de la Ville, et que, si la situation n’était pas rectifiée, le service de téléphone cellulaire pouvait être suspendu.

[9] [redacted]

À l’instar des tests réalisés avec un téléphone intelligent, les tests réalisés avec un ordinateur portatif de la Ville ont confirmé la mise en place d’importantes mesures de protection, notamment le cryptage, un accès administrateur restreint, ainsi que des antivirus et correctifs de systèmes d’exploitation à jour.

[redacted]

La vérification a aussi porté sur les contrôles d’authentification visant à confirmer l’identité des utilisateurs. L’authentification peut se faire au moyen d’une combinaison de facteurs; plus le nombre de facteurs requis est élevé, plus le contrôle est strict. Par exemple, demander un mot de passe obligatoire est une authentification à un facteur. Une authentification à deux facteurs pourrait être un mot de passe associé à un certificat numérique. Alors que celle à trois facteurs comprendrait également un paramètre biométrique (p. ex., empreinte digitale ou lecture rétinienne). [redacted]

Les mots de passe sont sujets au vol et à l’utilisation malveillante. [redacted] Les efforts de la Ville ne reflètent plus les normes de l’industrie et augmentent le risque que des utilisateurs non autorisés accèdent au réseau.

Dans le cadre des tests techniques, l’équipe de vérification a provoqué des incidents de sécurité au moyen de maliciels contenant un virus non fonctionnel pour déterminer si

[10] [redacted]

les technologies de sécurité de la Ville étaient capables de détecter et de bloquer les menaces. Si l’un des tests a été un succès, les autres n’ont pas permis de les détecter, de les signaler ou de les bloquer. Si la simulation avait été une réelle attaque, le réseau de la Ville aurait été à la merci du pirate informatique.

Surveillance et supervision

L’un des objectifs centraux est de prévenir les incidents de sécurité tout en offrant un accès à distance fiable et disponible. Malgré cela, il est presque certain que de tels incidents surviendront. Que ces derniers soient faits avec une mauvaise intention ou non, nos attentes étaient que la Ville ait recours à des mesures officielles et efficaces pour favoriser la détection et l’intervention en temps opportun et l’intensification de l’intervention dans le cas d’un incident de sécurité ou dans toute autre circonstance menaçant la disponibilité des services d’accès à distance. Par ailleurs, nous nous attendions à trouver un processus de supervision efficace dans le cadre duquel : les solutions d’accès à distance envisagées sont sujettes à une évaluation des risques et font l’objet d’analyses des vulnérabilités; les pratiques, les rôles et les responsabilités en matière de gestion des comptes d’accès à distance sont efficaces et appropriés; et le signalement efficace et rapide des incidents contribue à l’amélioration continue.

À l’instar de la vérification de la gestion d’un incident lié à la sécurité des TI et de l’intervention en la matière de 2015 du BVG, la présente vérification a révélé que la Ville possède des capacités de surveillance, de détection et d’intensification de l’intervention relativement aux incidents, y compris pour les applications d’accès à distance. Bien que ces capacités ne soient toujours pas à maturité, comme l’indiquait la vérification de 2015, on peut noter certains signes d’amélioration dans les deux dernières années. Par exemple, en 2016, la Ville a signé un contrat avec un nouveau fournisseur de services de sécurité gérés dans le but d’améliorer la prestation des services et la valeur ajoutée. Nous avons aussi constaté l’examen et la mise à jour exhaustifs du cadre stratégique en matière de TI de la Ville par les STI; notamment, la nouvelle norme sur la sécurité de l’information pour les services d’accès à distance (ISS-RAS) représente une grande possibilité d’amélioration en matière de supervision et de contrôle des solutions d’accès à distance, puisqu’elle impose des évaluations des risques. Point à noter : la vérification a constaté que des pratiques efficaces et officielles d’octroi des droits d’accès à distance étaient en place, et que les pratiques favorisant la bonne administration des comptes d’accès à distance – notamment, le rapprochement périodique des comptes des utilisateurs – avaient été améliorées.

Malgré ces améliorations, la vérification a soulevé certaines lacunes et faiblesses dans la capacité de la Ville à détecter les menaces à la sécurité et les vulnérabilités en matière d’accès à distance, et à y réagir. Plus précisément, la vérification a cerné les problèmes ci-dessous en matière de surveillance et de supervision.

- [redacted]
- Aucun test de pénétration précis n’a été mené pour des tiers connectés à partir d’un point éloigné afin de cibler les problèmes potentiels[11].

Ces problèmes sont décrits plus en détail ci-dessous.

En juin 2016, la Ville a signé un contrat avec un nouveau fournisseur de services de sécurité gérés. Durant la vérification, la Ville et son nouveau partenaire travaillaient toujours à instaurer le nouveau service. [redacted] Selon les normes de l’industrie, ce processus dure habituellement moins de trois (3) mois, soit beaucoup moins que l’expérience constatée à la Ville.

Les cas pratiques décrivent des scénarios de vulnérabilité précis que le fournisseur de services de sécurité gérés aurait à détecter dans ses activités de surveillance. Ils servent aussi de référence quant à la nature et à la portée des registres des activités et des types d’activités relatifs à l’accès à distance (ou « trafic ») que le fournisseur de services de sécurité gérés doit surveiller. Des cas pratiques normalisés ont été instaurés, conformément au contrat avec la Ville. [redacted]

[11] Cette même observation a été faite dans la vérification de la gestion des incidents liés à la sécurité des TI et des interventions en la matière de 2015, qui recommandait que le CI mène des tests de pénétration dans toutes les infrastructures essentielles.

Dans le cadre de ses tests techniques, l’équipe de vérification a analysé les vulnérabilités des serveurs d’accès à distance de la Ville. Ces analyses n’ont pas permis de détecter des lacunes majeures, mais elles ne sont pas conçues pour offrir le même degré d’assurance qu’une analyse des vulnérabilités ciblée ou un test de pénétration menés par un tiers. On note, à l’instar des constatations de la vérification de la gestion d’un incident lié à la sécurité des TI et de l’intervention en la matière de 2015, qu’aucune analyse des vulnérabilités et aucun test de pénétration réguliers n’étaient menés[12] pour l’ensemble des solutions d’accès à distance des directions générales et de la Ville. Des entretiens avec le personnel des STI révèlent par ailleurs qu’habituellement, les STI mènent des évaluations des risques au cas par cas, selon le degré de risque perçu. Cette lacune est résolue par la nouvelle norme sur la sécurité de l’information pour les services d’accès à distance (ISS-RAS), qui exige que les technologies d’accès à distance fassent l’objet d’une analyse des vulnérabilités deux fois par année, et d’une évaluation des risques ou des menaces, au moins tous les trois ans. Comme l’indique la recommandation n^{o} 2, le personnel est invité à mettre en œuvre cette nouvelle norme aussitôt que possible.

Selon les entretiens et les examens de documents menés durant la vérification, le rapprochement des comptes d’accès à distance[13] (ceux fournis à des employés ne travaillant pas pour la Ville) n’avait pas été réalisé dans des délais raisonnables. Cependant, au cours du processus de vérification, les STI ont commencé à vérifier leur banque de données de tiers ayant un accès à distance pour s’assurer que ces derniers avaient toujours besoin d’un accès, et que les renseignements pertinents étaient exacts et à jour (p. ex., date de fin de contrat et nom de la personne-ressource dans le secteur d’activités de la Ville). L’équipe de vérification comprend que cette amélioration dans l’administration des comptes d’accès à distance devra se traduire par des vérifications périodiques pour veiller à limiter l’accès aux comptes aux seuls utilisateurs appropriés et autorisés.

[12] L’équipe de vérification notait que la nouvelle solution de VPN Citrix, dont la mise en œuvre est prévue en 2017, avait fait l’objet d’une évaluation de la vulnérabilité.

[13] Il s’agit de comptes de personnes qui ne travaillent pas à la Ville, notamment des entrepreneurs et fournisseurs qui, dans leurs fonctions, ont besoin d’un accès à distance.

Recommandations et réponses

Recommandation nº 1

Le CI devrait s’assurer que la stratégie de la Ville en matière de TI permet d’offrir un accès à distance à toutes les directions générales et pour tous les services. Cette stratégie doit tenir compte de la manière dont les différentes directions générales assurent la connexion et la sécurité de l’accès à distance pour les services névralgiques. Par ailleurs, elle doit aborder les mesures à prendre dans la foulée des vérifications antérieures des TI, le cas échéant.

Réponse de la direction

La direction approuve cette recommandation. Le CI fera le nécessaire pour intégrer l’accès à distance pour tous les services et directions générales dans la stratégie en matière de TI d’ici le T2 de 2018.

Recommandation nº 2

La Ville devrait veiller à l’adoption de la nouvelle norme relative à l’accès à distance, et voir à ce que toutes les directions générales de la Ville acceptent que le service en matière de sécurité soit centralisé. La norme devrait clairement définir la portée et les limites de l’environnement informatique de la Ville.

Réponse de la direction

La direction approuve cette recommandation. L’autorité responsable de la gestion des risques liés à la sécurité technologique veillera à ce que la norme sur la sécurité de l’information pour les services d’accès à distance (ISS-RAS) soit adoptée dans toutes les directions générales de la Ville et administrée à titre de service organisationnel par une autorité centrale en matière de sécurité d’ici le T2 de 2018.

Recommandation nº 3

La Ville devrait prendre des mesures pour que l’examen et la mise à jour de ses politiques en matière de TI aient lieu au moins tous les deux (2) ans.

Réponse de la direction

La direction approuve cette recommandation. Le CI fera le nécessaire afin que d’ici le T4 de 2018, toutes les politiques soient revues, après quoi un autre cycle de deux ans sera enclenché.

Recommandation nº 4

La Ville devrait élaborer et tenir à jour un document ou un diagramme décrivant concrètement l’architecture du réseau des TI de la Ville, soit pour toutes les directions générales et pour tous les services. Les changements à l’architecture devraient être approuvés par le CI.

Réponse de la direction

La direction approuve cette recommandation. Le CI fera le nécessaire pour consigner, d’ici le T3 de 2018, l’architecture du réseau municipal touchant tous les services et directions générales, et pour tenir à jour ce document. Les modifications de l’architecture feront l’objet d’un processus d’évaluation avant d’être approuvées.

Recommandation nº 5

Comme un grand nombre d’intervenants, de directions générales et de services accèdent à distance au réseau de la Ville, cette dernière devrait créer un registre centralisé de toutes les solutions de connexion à distance utilisées au sein des directions générales et de la Ville. Ce registre devrait définir le type d’accès à distance, indiquer comment il est isolé des réseaux des autres services de la Ville (ou connecté à ces derniers) et établir les facteurs à considérer ou les exigences en matière de sécurité. Les changements proposés au registre devraient être approuvés par le CI.

Réponse de la direction

La direction approuve cette recommandation. Le CI mettra en place un processus pour consigner les solutions d’accès à distance, ainsi que leurs caractéristiques et les liens entre elles, pour toutes les directions générales de la Ville. Sera également mis sur pied un mécanisme de suivi, de surveillance et d’approbation des changements aux solutions consignées, d’ici le T1 de 2019.

Recommandation nº 6

La Ville devrait prendre les mesures nécessaires pour mieux gérer les appareils mobiles, entre autres en instaurant des exigences et des mesures de contrôle techniques additionnelles en matière de sécurité pour l’accès à distance.

- [redacted]
- [redacted]

Réponse de la direction

La direction approuve cette recommandation. Le CI mettra en œuvre les mesures de contrôle [redacted] pour les connexions à distance. [redacted] Ce sera fait d’ici le T4 de 2019.

Recommandation nº 7

La Ville devrait évaluer et améliorer la gestion et la surveillance de la sécurité de l’accès à distance, en prenant notamment la mesure suivante :

- [redacted]
- Continuer d’améliorer les pratiques opérationnelles, entre autres la gestion et le rapprochement des comptes des fournisseurs et des employés.

Réponse de la direction

La direction approuve cette recommandation. [redacted] Des mesures opérationnelles seront prises afin d’améliorer la gestion des comptes des fournisseurs et de veiller au maintien des activités de rapprochement des comptes, d’ici le T4 de 2019.

Conclusion

Ottawa est une ville moderne et connectée dont la dépendance aux technologies de l’information et de communication s’accroît de plus en plus. Protéger le réseau et les infrastructures technologiques essentielles de la Ville contre l’accès à distance non autorisé est un élément central d’une stratégie de cybersécurité efficace. Le présent rapport de vérification décrit des faiblesses et des lacunes qui exposent la Ville à différents risques potentiellement importants en matière de sécurité des TI, de fiabilité et de prestation des services. [redacted]

Vu le rythme avec lequel les technologies évoluent et la dépendance accrue de la Ville à l’accès à distance, il est important de donner suite rapidement aux recommandations du présent rapport, ainsi qu’aux recommandations complémentaires formulées dans les vérifications antérieures en matière de TI.

Malgré les problèmes et les risques associés soulevés précédemment, nous reconnaissons que la Ville offre un accès à distance ayant un degré élevé de disponibilité, et qu’elle a pris l’initiative d’améliorer certains volets des mesures de contrôle, de la gestion des risques et de la gouvernance. Ces initiatives comprennent l’élaboration d’une nouvelle norme sur la sécurité de l’information qui contribuera à résoudre les problèmes récurrents associés à l’absence d’une autorité centrale assumant la responsabilité de la gestion des risques relatifs à l’accès à distance.

Rapport de vérification détaillé

Vérification de l’accès à distance aux TI

Introduction

La vérification de l’accès à distance aux TI figurait dans le Plan de vérification de 2016 du Bureau du vérificateur général (BVG), approuvé par le Conseil municipal en novembre 2015.

Renseignements généraux et contexte

Comme la plupart des organisations, la Ville d’Ottawa (la « Ville ») s’appuie de plus en plus sur la technologie pour atteindre une multitude d’objectifs stratégiques et opérationnels. L’une des nombreuses avancées technologiques des dernières années est la possibilité, pour les employés municipaux et autres utilisateurs autorisés, d’accéder au réseau des technologies de l’information (TI) à partir d’appareils autres que les postes de travail des bureaux municipaux. Cet accès a grandement amélioré l’efficacité du travail pour différents utilisateurs et dans de nombreuses situations opérationnelles. L’accès à distance n’est plus considéré comme une option, mais bien comme un outil essentiel du quotidien servant à répondre aux besoins en matière de TI des travailleurs mobiles (comme les paramédics et les agents des règlements), des fournisseurs (ceux qui en ont besoin pour voir à la maintenance et à la surveillance des applications et des systèmes) et des télétravailleurs, pour ne nommer que ceux-là.

Les besoins opérationnels et les avantages de l’accès à distance se multiplient, et les risques qui y sont associés s’accroissent également. En effet, vu la prolifération de certaines technologies, comme les téléphones intelligents, et le foisonnement des options d’accès à distance, le risque d’accès non autorisé est de plus en plus grand. Les accès non autorisés pourraient entraîner différentes répercussions, comme la perte ou la corruption de données, la divulgation de renseignements confidentiels ou privés et des interruptions de service. Dans cet environnement, la Ville doit agir de façon proactive pour gérer les risques et les possibilités en matière de nouvelles technologies. Une telle approche comprend l’adoption de mesures visant à trouver un équilibre entre les avantages opérationnels et la nécessité d’assurer la sécurité des technologies et outils d’accès à distance actuels et futurs, au moyen de politiques, d’exigences, de lignes directrices et de pratiques.

La Ville a instauré un cadre stratégique et des exigences pour régir l’accès à distance, notamment la Politique sur l’utilisation responsable des ordinateurs, la Politique sur la sécurité des informations, la Politique sur les appareils technologiques et le Code de conduite du personnel. Figurant parmi les politiques en matière de TI, la Politique sur l’accès à distance au réseau de la Ville, instaurée en 2006, vise tous les employés de la Ville qui ont besoin d’un accès à distance. Cette politique, dont la dernière mise à jour remonte à 2012, définit les responsabilités des utilisateurs, les processus d’autorisation et les mécanismes de sécurité permettant au personnel autorisé d’accéder à distance au réseau de la Ville. Elle décrit aussi l’offre de services[14] des Services de technologie de l’information (STI) de la Ville qui visent à soutenir l’accès à distance. Au moment de la vérification, les STI réalisaient un examen et une mise à jour exhaustifs du cadre stratégique en matière de TI, qui comprend la Politique sur l’accès à distance au réseau de la Ville. L’initiative a mené à la proposition d’un certain nombre de normes de sécurité technologique, notamment la nouvelle norme sur la sécurité de l’information pour les services d’accès à distance (Information Security Standard – Remote Access Services [ISS-RAS]). Comme il est expliqué plus loin, cette norme pallie certaines lacunes importantes du cadre stratégique actuel et clarifie les responsabilités et les pouvoirs du chef de l’information (CI). Ce dernier point est particulièrement important étant donné les solutions d’accès à distance personnalisées en usage dans différents secteurs comme OC Transpo, les Services d’eau, les Services de la circulation et la Bibliothèque publique d’Ottawa, qui ont recours à une équipe de TI autonome. Au moment de la production du présent rapport de vérification, la nouvelle norme n’avait pas encore été mise en œuvre.

Comme il est mentionné précédemment et décrit plus en détail dans le présent document, certains problèmes de gouvernance – notamment à propos des rôles, des responsabilités et des pouvoirs – ont mené à différentes observations lors de la vérification. Dans les dernières années, le Bureau du vérificateur général (BVG) a mené différentes vérifications des TI grâce auxquelles il a détecté différents problèmes de gouvernance, qui ont mené à un grand nombre des conclusions et recommandations du présent rapport. Les vérifications réalisées antérieurement sont la vérification de la gouvernance des TI (2014), la vérification de la gestion des risques liés aux TI (2015) et la vérification de la gestion des incidents liés à la sécurité des TI et des interventions en la matière (2015). Chacune de ces vérifications a permis de cibler des facteurs de

[14] Les services suivants sont décrits dans la Politique sur l’accès à distance au réseau de la Ville : Web Mail, BlackBerry™, réseau privé virtuel (accès à partir d’un ordinateur portatif de la Ville) et les postes de travail à distance (accès à partir de l’ordinateur personnel d’un employé).

risque liés à des technologies ou des systèmes exclusifs gérés par des équipes de TI autonomes[15] plutôt que ceux gérés de façon centralisée par les STI. C’est pourquoi il est difficile pour la Ville de promouvoir des stratégies et des exigences relatives aux TI uniformes à l’échelle de l’organisation, y compris celles liées à la sécurité. De plus, ces vérifications ont permis de relever un manque de continuité systémique associé au poste de CI. Même si la vérification faisant l’objet du présent rapport ne se voulait pas un suivi des vérifications antérieures, mentionnons que ces deux problèmes sont toujours présents en 2017. Ils contribuent à accroître les risques relatifs à l’accès à distance et ont mené à bon nombre des conclusions et des recommandations du présent rapport. Au cours de la vérification, le BVG a informé les STI des points communs entre les vérifications antérieures et les conclusions et résultats de la présente vérification, et les a encouragés à donner suite avec diligence aux recommandations précédemment formulées. Conformément au protocole de vérification de la Ville, le BVG continue de prendre des mesures pour assurer le suivi actif de la réponse des STI aux conclusions des vérifications antérieures.

Approche et méthodologie de la vérification

La vérification visait surtout à évaluer de façon indépendante la pertinence et l’efficacité des systèmes, des pratiques et des procédures, et de la gouvernance en place, afin de détecter et de réduire les risques associés à l’accès à distance au réseau de la Ville, notamment en matière de sécurité. Les éléments prioritaires sont les suivants :

- Recours à l’accès à distance;
- Rôles et responsabilités pour octroyer le droit d’accès;
- Architecture et technologie pour l’accès à distance;
- Fonctionnement et surveillance de l’accès à distance.

Des critères de vérification (voir l’annexe A *Objectifs et critères de la vérification*) ont été établis en fonction des principaux guides en matière d’accès à distance aux TI, comme ceux publiés par le National Institute of Standards and Technology (NIST). Plus

[15] Comme il est indiqué plus loin dans le présent rapport, l’existence d’équipes de TI autonomes ne signifie pas que les STI ne participent pas à la gestion des systèmes et technologies exclusifs, mais bien que leur participation ne se fait pas à titre d’autorité officielle.

précisément, les publications spéciales 800-46[16] et 800-53[17] du NIST, ainsi que des éléments pertinents de son cadre de cybersécurité[18] ont grandement éclairé les critères de vérification.

Portée

La présente vérification portait sur les différents types d'accès à distance[19] offerts aux utilisateurs :

1. Les réseaux privés virtuels (VPN), par exemple :
    a. Protocole de sécurité IP (IPsec);
    b. Liens cryptés (protocole SSL);
2. Connexions par contrôle à distance (par exemple Citrix et les solutions de bureau à distance);
3. La connectivité mobile (par exemple BlackBerry™, autres téléphones intelligents, tablettes);
4. L'accès à distance sur le Web (par exemple Outlook Web Access).

L'examen visait aussi les mesures de contrôle au sein des STI et dans l'ensemble des secteurs d'activités et directions générales qui offrent un accès à distance, y compris les secteurs qui ont une équipe de TI autonome.

Il faut préciser que l'évaluation ne portait pas sur les réseaux privés virtuels (VPN) pour le travail à distance et l'accès par les membres du Conseil.

Approche et méthodologie de la vérification

La vérification a été conçue et menée conformément aux normes de vérification de la Ville pour que les procédures utilisées soient suffisantes et appropriées et pour que les

[16] *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security,* 2016, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

[17] *Security and Privacy Controls for Federal Information Systems and Organizations,* 2013 (version mise à jour en 2015), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[18] *Framework for Improving Critical Infrastructure Cybersecurity,* 2014,

https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[19] La vérification ne comprenait pas l'accès aux passerelles d'accès ou de communication qui ne sont pas reliées directement au réseau de la Ville (p. ex., systèmes radio ou autres systèmes de communication).

renseignements recueillis assurent de façon raisonnable l’exactitude des conclusions au moment où la vérification a eu lieu.

L’approche était axée sur une évaluation de l’accès à distance aux TI à l’échelle de la Ville. L’équipe de vérification a examiné les politiques, les procédures et les pratiques en matière d’accès à distance aux TI au sein des STI et dans la Ville en général pour déterminer si leur conception était adéquate et leur mise en œuvre était efficace.

Des examens de documents, des entrevues et des tests ont été effectués durant la période de vérification (de janvier à mai 2016), notamment des tests techniques, dans le cadre desquels les STI ont fourni un ordinateur portatif Windows et un téléphone BlackBerry™ correspondant aux normes de la Ville à l’équipe de vérification. Cette dernière a testé ces appareils et les a utilisés pour se connecter aux services d’accès à distance de la Ville. Ont été examinés et évalués dans le cadre des tests techniques :

- les contrôles de sécurité des points terminaux (p. ex., prévention et détection des maliciels);
- la sécurité de l’isolation des systèmes d’accès à distance des directions générales (pour veiller à ce que les systèmes essentiels soient isolés du réseau de la Ville);
- le soutien et la disponibilité (p. ex., pour les pratiques opérationnelles et les mises à jour courantes);
- la surveillance opérationnelle et la détection des incidents (p. ex., les alertes en cas d’incident de sécurité).

Observations et recommandations de l’équipe de vérification

La présente section décrit les principales observations tirées de la vérification et, le cas échéant, les recommandations applicables.

Stratégie relative à la technologie d’accès à distance

Dans la vérification de la gouvernance des TI de 2014 du BVG, on notait que la Ville avait produit la *Feuille de route technologique,* qui cernait les priorités, les initiatives et les objectifs en matière de TI. Or, on relevait aussi un manque d’harmonisation entre les investissements dans les TI de la Ville et ses priorités stratégiques et opérationnelles. La présente vérification révèle que la Ville n’a toujours pas résolu ces problèmes et n’a pas mis à jour la *Feuille de route technologique 2013-2016.* Elle confirme en outre qu’il n’existe aucune stratégie officielle qui orienterait les priorités et la prise de décision de

la Ville en matière d'accès à distance et clarifierait les responsabilités à l'égard des risques relatifs à l'accès à distance et la manière de les gérer.

Bien que les STI disent élaborer actuellement une nouvelle stratégie en matière de TI, ils n'ont pas l'intention d'y inclure ou de créer une stratégie relative à la technologie d'accès à distance qui orienterait les priorités et la prise de décision de la Ville en matière d'accès à distance tout en les articulant autour d'une vision claire[20]. L'absence d'une stratégie officielle augmente les risques de failles et de disparités dans les pratiques et les technologies d'accès à distance à l'échelle de la Ville et contribue aux problèmes déjà soulevés en ce qui a trait :

- à la responsabilité à l'égard des risques relatifs à l'accès à distance qui menacent la sécurité du réseau et gestion de ces risques;
- aux rôles, aux responsabilités et à la reddition de comptes;
- à la gouvernance et à la prise de décision.

Même si la vérification a permis d'établir que les rôles, les responsabilités et la reddition de comptes sur le plan opérationnel (p. ex., administration des comptes d'accès à distance, approbations et évaluation des risques) sont généralement clairs et font souvent l'objet de procédures et de listes de vérification officielles, certains problèmes ont été relevés à l'échelon supérieur. Plus précisément, la responsabilité à l'égard des risques relatifs à l'accès à distance de la Ville, de même que les rôles, les responsabilités et la reddition de comptes ne sont pas clairement établis au sein des différentes directions générales et de la Ville. Cette observation concorde avec les conclusions de la vérification de la gestion des risques liés aux TI de 2015 du BVG, qui soulevait des problèmes similaires concernant l'autorité et les responsabilités du chef de l'information à l'égard des risques relatifs aux TI à l'échelle de la Ville. Cette vérification a permis au BVG de conclure que les STI jouent un rôle efficace et approprié dans la surveillance[21], la supervision et la réduction des risques relatifs à l'accès à distance. Ce rôle comprend la création d'outils et de pratiques permettant de veiller au respect des normes, protocoles et autres exigences de la Ville, notamment

[20] Cette vision permettrait de formuler une approche efficace et globale en matière d'accès à distance qui assurerait un équilibre entre les besoins opérationnels et les exigences de sécurité et coordonnerait la planification et la prise de décision dans des domaines émergents, comme les technologies mobiles et le concept « apportez votre propre appareil ».

[21] Le suivi de la conformité est une responsabilité partagée de chaque direction générale (p. ex., suivi des comptes de personnes ne travaillant pas pour la Ville) et des STI (p. ex., suivi des comptes inactifs à l'échelle de la Ville).

lors du choix et de la mise en place des technologies d’accès à distance, de l’octroi de connexions à distance aux employés et aux fournisseurs et de l’administration des comptes. Cependant, leur rôle ne s’étend pas officiellement au déploiement de l’accès à distance dans les directions générales où cet accès est géré par une équipe de TI autonome, ce qui, selon les vérifications antérieures du BVG, peut représenter un problème. Pour procéder à ces déploiements, la participation des STI à tous les volets de l’initiative – y compris dans la prise de décision névralgique – peut être soit minime, voire absente, soit très importante. Cette situation persistante limite la capacité des STI d’adopter une vision globale des technologies d’accès à distance de la Ville qui lui permettrait de soutenir une planification économique et opérationnelle stratégique et efficace, ainsi qu’une bonne gestion des risques.

Si la vérification a permis de relever des problèmes associés à l’absence d’une stratégie relative à la technologie d’accès à distance à l’échelle de la Ville pour orienter efficacement sa vision, elle a aussi permis de noter l’existence d’un certain nombre d’initiatives pour aider à les résoudre. Comme il est indiqué dans la section *Renseignements généraux et contexte,* les STI effectuent actuellement un examen et une mise à jour exhaustifs du cadre stratégique en matière de TI de la Ville. L’examen et la mise à jour comprendront le remplacement de la Politique sur l’accès à distance au réseau de la Ville actuelle, jugée désuète et largement inefficace. La nouvelle norme sur la sécurité de l’information pour les services d’accès à distance semble offrir une bonne couverture technique pour satisfaire aux exigences de l’accès à distance – notamment en matière de suivi, de tests et d’application de correctifs – et formule des attentes claires pour les utilisateurs finaux relativement à l’utilisation appropriée. De plus, la version provisoire de la norme indique clairement qu’elle s’applique à tous les services qui offrent une connexion à distance aux environnements informatiques de la Ville, notamment ceux gérés par des équipes de TI autonomes ou des tiers. Par ailleurs, elle clarifie l’obligation de faire approuver par le CI toute exemption aux obligations inhérentes à la norme. Voilà des éléments importants qui aideront à résoudre les problèmes soulevés dans la présente vérification et les vérifications antérieures[22]. L’approbation et la mise en œuvre de la nouvelle norme (en version provisoire depuis 2016) constitueront des étapes clés pour corriger les lacunes actuelles en matière de contrôle et d’uniformité de l’accès à distance à l’échelle de la Ville.

[22] Comme il est indiqué précédemment, la présente vérification ne se voulait pas un suivi des vérifications des TI antérieures du BVG.

Recommandation nº 1

Le CI devrait s’assurer que la stratégie de la Ville en matière de TI permet d’offrir un accès à distance à toutes les directions générales et pour tous les services. Cette stratégie doit tenir compte de la manière dont les différentes directions générales assurent la connexion et la sécurité de l’accès à distance pour les services névralgiques. Par ailleurs, elle doit aborder les mesures à prendre dans la foulée des vérifications antérieures des TI, le cas échéant.

Réponse de la direction

La direction approuve cette recommandation. Le CI fera le nécessaire pour intégrer l’accès à distance pour tous les services et directions générales dans la stratégie en matière de TI d’ici le T2 de 2018.

Recommandation nº 2

La Ville devrait veiller à l’adoption de la nouvelle norme relative à l’accès à distance, et voir à ce que toutes les directions générales de la Ville acceptent que le service en matière de sécurité soit centralisé. La norme devrait clairement définir la portée et les limites de l’environnement informatique de la Ville.

Réponse de la direction

La direction approuve cette recommandation. L’autorité responsable de la gestion des risques liés à la sécurité technologique veillera à ce que la norme sur la sécurité de l’information pour les services d’accès à distance (ISS-RAS) soit adoptée dans toutes les directions générales de la Ville et administrée à titre de service organisationnel par une autorité centrale en matière de sécurité d’ici le T2 de 2018.

Recommandation nº 3

La Ville devrait prendre des mesures pour que l’examen et la mise à jour de ses politiques en matière de TI aient lieu au moins tous les deux (2) ans.

Réponse de la direction

La direction approuve cette recommandation. Le CI fera le nécessaire afin que d’ici le T4 de 2018, toutes les politiques soient revues, après quoi un autre cycle de deux ans sera enclenché.

Architecture pour l’accès à distance – Inventaire et flux de données

Vu l’importance accrue de l’accès à distance pour soutenir les activités opérationnelles, y compris certaines fonctions essentielles, les vérificateurs s’attendaient à trouver une architecture organisationnelle d’accès à distance mise par écrit pour donner une vision d’ensemble de tous les types de connexion à distance offerts par la Ville. Un tel document donnerait des renseignements sur 1) la connexion entre les appareils d’accès à distance de toutes les directions générales de la Ville et les STI; 2) les technologies d’accès à distance en place, notamment celles relatives au SCADA ou aux applications exclusives avec connexion à distance; 3) les flux de données associés.

Or, la vérification a révélé que la Ville n’a consigné ni son architecture, ni l’inventaire exhaustif de ses technologies, connexions et flux de données relatifs à l’accès à distance, y compris dans les cas de déploiements par des directions générales. Malgré l’absence d’une architecture organisationnelle, on peut trouver des documents sur l’architecture de certains services d’accès à distance de la Ville (infrastructure VPN ou BlackBerry™, connexion pour bureau à distance, etc.) ainsi qu’un inventaire des ordinateurs portatifs et téléphones intelligents appartenant à la Ville. De plus, l’équipe de vérification sait que les STI ont récemment conçu des plans et assigné certaines responsabilités en vue de créer un répertoire central des risques et des technologies relatifs à l’accès à distance. Cependant, au moment de la vérification, l’absence d’un inventaire organisationnel exhaustif entraînait certaines répercussions pour la Ville, notamment l’incapacité à élaborer une planification stratégique efficace et à en tirer profit. Sans planification stratégique, les investissements dans les technologies, les services et les procédures en matière d’accès à distance risquent d’être moins bien coordonnés pour optimiser les ressources et la sécurité. Sur le plan opérationnel, cette lacune augmente la probabilité de différents problèmes : atteintes à la sécurité ou violation de règlements (p. ex. sur la vie privée) en raison de connexions à distance non conformes, retards dans la détection de ces atteintes ou violations, et utilisation de plateformes d’accès à distance non autorisées. Enfin, une mise en œuvre efficace de la nouvelle norme sur la sécurité de l’information pour les services d’accès à distance nécessite également une définition et une démarcation claires de l’environnement informatique de la Ville, conformément à ladite norme (voir la recommandation nº 2).

Recommandation nº 4

> La Ville devrait élaborer et tenir à jour un document ou un diagramme décrivant concrètement l’architecture du réseau des TI de la Ville, soit pour toutes les

directions générales et pour tous les services. Les changements à l’architecture devraient être approuvés par le CI.

Réponse de la direction

La direction approuve cette recommandation. Le CI fera le nécessaire pour consigner, d’ici le T3 de 2018, l’architecture du réseau municipal touchant tous les services et directions générales, et pour tenir à jour ce document. Les modifications de l’architecture feront l’objet d’un processus d’évaluation avant d’être approuvées.

Recommandation nº 5

Comme un grand nombre d’intervenants, de directions générales et de services accèdent à distance au réseau de la Ville, cette dernière devrait créer un registre centralisé de toutes les solutions de connexion à distance utilisées au sein des directions générales et de la Ville. Ce registre devrait définir le type d’accès à distance, indiquer comment il est isolé des réseaux des autres services de la Ville (ou connecté à ces derniers) et établir les facteurs à considérer ou les exigences en matière de sécurité. Les changements proposés au registre devraient être approuvés par le CI.

Réponse de la direction

La direction approuve cette recommandation. Le CI mettra en place un processus pour consigner les solutions d’accès à distance, ainsi que leurs caractéristiques et les liens entre elles, pour toutes les directions générales de la Ville. Sera également mis sur pied un mécanisme de suivi, de surveillance et d’approbation des changements aux solutions consignées, d’ici le T1 de 2019.

Lacunes relatives à la sécurité de l’accès à distance aux TI

Bien qu’il soit essentiel sur le plan opérationnel d’offrir une connexion à distance fiable et hautement disponible dans l’environnement actuel, cette connexion pose certains risques quant à la sécurité des TI, notamment sur le plan de la confidentialité, de l’intégrité et de la disponibilité. Pour réduire et gérer ces risques, il faut que les pratiques et les mesures de contrôle en matière de sécurité permettent de prévenir et de détecter les incidents relatifs à l’accès à distance non autorisé au moyen des différents outils (VPN, bureau à distance, téléphones intelligents, etc.), puis d’y réagir. Il faudrait aussi qu’elles prennent en compte les exigences opérationnelles de la Ville et la

nécessité des mesures de sécurité adéquates. Dans son examen des mesures de sécurité, les vérificateurs ont tenu compte des contextes ci-dessous.

- Points terminaux (c.-à-d. ordinateurs portatifs ou téléphones intelligents utilisés pour accéder au réseau de la Ville) – les appareils doivent être configurés et protégés de façon à empêcher l’accès non autorisé et toute autre activité posant un risque. Pour être sécuritaire, un point terminal doit être crypté, demander un mot de passe sécuritaire, assurer une protection contre les maliciels et être géré de façon centralisée avec une configuration verrouillée.
- Architecture du réseau – la Ville doit prévenir l’accès à distance non autorisé au réseau de la Ville. La conception du réseau et l’architecture doivent permettre aux directions générales dont l’infrastructure est essentielle de s’isoler de l’accès à distance par le réseau de la Ville.
- Services de soutien – le soutien aux utilisateurs de l’accès à distance devrait être très disponible (p. ex., après les heures normales de bureau), être soumis à des mesures de sécurité appropriées (p. ex., validation de l’identité de l’utilisateur avant la prestation du service) et respecter les normes.
- Surveillance opérationnelle et détection d’incidents – la surveillance des activités et du trafic relatifs à l’accès à distance devrait permettre de relever les anomalies, les alertes et les problèmes potentiels de sécurité, et, le cas échéant, de procéder à l’intensification de l’intervention. Les mesures de contrôle examinées par les vérificateurs comprennent celles imparties par la Ville à un fournisseur de services de sécurité gérés.

Dans le cadre de la vérification, l’équipe a examiné les mesures de sécurité mentionnées précédemment par une série de tests techniques : utilisation d’un ordinateur portatif et d’un BlackBerry™ de la Ville pour se connecter à distance au réseau, et utilisation d’appareils n’appartenant pas à la Ville pour tester l’accès non autorisé au réseau et aux fonctionnalités de la Ville.

Les tests réalisés avec des appareils fournis par la Ville ont permis de constater qu’un certain nombre de mesures de sécurité efficaces sont en place et de confirmer la résilience des systèmes d’accès à distance et leur capacité à offrir une grande disponibilité. Les vérificateurs ont noté que l’architecture par défaut permet d’isoler les infrastructures essentielles du réseau général de la Ville. Concernant les mesures de sécurité précises, l’ordinateur portatif fourni par la Ville était beaucoup plus sécuritaire que le téléphone intelligent. L’ordinateur portatif offrait un contrôle efficace pour prévenir le contournement des restrictions (p. ex., mots de passe) ou le rehaussement non autorisé du niveau d’accès d’un utilisateur. De plus, l’ordinateur portatif était configuré

avec un logiciel de sécurité à jour, son disque dur était entièrement crypté et il ne permettait pas l’exportation non autorisée d’un logiciel VPN sur un ordinateur portatif n’appartenant pas à la Ville.

L’équipe de vérification a réussi à obtenir d’autres résultats positifs à la suite de ses tests. Elle a notamment constaté que l’architecture du réseau d’accès à distance semblait peu vulnérable aux tentatives d’accès non autorisé. De même, les utilisateurs autorisés se voyaient imposer certaines restrictions relativement à l’accès et aux fonctionnalités lorsqu’ils se connectaient à distance à partir d’appareils n’appartenant pas à la Ville. De plus, les tests ont permis de conclure que la Ville avait mis en place des procédures opérationnelles de gestion de l’accès à distance appropriées pour l’utilisateur final et pour la bonne administration des comptes.

Cependant, les tests ont aussi révélé des problèmes en raison de certaines lacunes et faiblesses relatives à l’environnement de sécurité pour l’accès à distance. Celles-ci pourraient compromettre la capacité de la Ville à prévenir et à détecter les incidents, dont l’accès non autorisé, et à y réagir. Plus précisément, la vérification a permis de relever les problèmes techniques suivants en matière de sécurité de l’accès à distance :

- Les appareils mobiles fournis par la Ville ne sont pas suffisamment sécuritaires;
- [redacted]
- [redacted]
- La surveillance en matière de sécurité n’a pas été optimisée pour cibler les scénarios d’atteinte à la sécurité lors d’une connexion à distance et y réagir.

Ces problèmes sont décrits plus en détail ci-dessous.

Lors de la vérification, les tests réalisés avec un téléphone intelligent de la Ville ont révélé que l’appareil mobile était configuré avec le plus récent système d’exploitation de BlackBerry™ et différentes mesures de sécurité, notamment la technologie BlackBerry Balance, servant à séparer les espaces professionnel et personnel. Par ailleurs, le système de gestion des appareils de la Ville envoie une alerte par courriel aux utilisateurs dès la détection d’activités anormales[23]. Cependant, l’appareil n’était pas suffisamment sécuritaire pour pallier les faiblesses et lacunes relevées. [redacted]

[23] Dans ce cas, l’alerte indiquait que l’appareil n’était plus conforme aux politiques et paramètres de sécurité visant à protéger les renseignements et le réseau de la Ville, et que, si la situation n’était pas rectifiée, le service de téléphone cellulaire pouvait être suspendu.

- [redacted]
- [redacted][24]
- [redacted]

[redacted]

À l’instar des tests réalisés avec un téléphone, les tests réalisés avec un ordinateur portatif de la Ville ont confirmé la mise en place d’importantes mesures de protection, notamment le cryptage, un accès administrateur restreint, ainsi que des antivirus et correctifs de systèmes d’exploitation à jour.

[redacted][25]

La vérification a aussi porté sur les contrôles d’authentification visant à confirmer l’identité des utilisateurs. L’authentification peut se faire au moyen d’une combinaison de facteurs; plus le nombre de facteurs requis est élevé, plus le contrôle est strict. Par exemple, demander un mot de passe obligatoire est une authentification à un facteur. Un deuxième facteur pourrait être un certificat numérique, et un troisième, un paramètre biométrique (p. ex., empreinte digitale ou lecture rétinienne). [redacted]

[redacted]

Les mots de passe sont susceptibles de vol et d’utilisation malveillante. [redacted] ne correspondent plus aux normes de l’industrie et augmentent les risques d’accès au réseau par des utilisateurs non autorisés.

Dans le cadre des tests techniques, l’équipe de vérification a provoqué des incidents de sécurité au moyen de maliciels contenant un virus non fonctionnel pour déterminer si les technologies de sécurité de la Ville étaient capables de détecter et de bloquer les menaces. Si l’un des tests a été un succès, les autres n’ont pas permis de les détecter, de les signaler ou de les bloquer.

Recommandation nº 6

La Ville devrait prendre les mesures nécessaires pour mieux gérer les appareils mobiles, entre autres en instaurant des exigences et des mesures de contrôle techniques additionnelles en matière de sécurité pour l’accès à distance.

- [redacted]
- [redacted]

Réponse de la direction

La direction approuve cette recommandation. Le CI mettra en œuvre les mesures de contrôle [redacted] pour les connexions à distance. [redacted] Ce sera fait d’ici le T4 de 2019.

Surveillance et supervision

L’un des objectifs centraux est de prévenir les incidents de sécurité tout en offrant un accès à distance fiable et disponible. Malgré cela, il est presque certain que de tels incidents surviendront. Que ces derniers soient le fait d’une personne mal intentionnée ou non, nos attentes étaient que la Ville ait recours à des mesures officielles et

efficaces pour favoriser la détection, l’intervention et l’intensification rapides dans le cas d’un incident de sécurité ou dans toute autre circonstance menaçant la disponibilité des services d’accès à distance. Par ailleurs, nous nous attendions à trouver un processus de supervision efficace dans le cadre duquel : les solutions d’accès à distance sont sujettes à une évaluation des risques et font l’objet d’analyses des vulnérabilités; les pratiques, les rôles et les responsabilités en matière de gestion des comptes d’accès à distance sont efficaces et appropriés; et le signalement efficace et rapide des incidents contribue à l’amélioration continue.

À l’instar de la vérification de la gestion des incidents liés à la sécurité des TI et des interventions en la matière de 2015 du BVG, la présente vérification a révélé que la ville possède des capacités de surveillance, de détection et d’intensification de l’intervention relativement aux incidents, y compris pour les applications d’accès à distance. Bien que ces capacités n’aient pas encore atteint leur maturité, comme l’indiquait la vérification de 2015, on peut noter certains signes d’amélioration dans les deux dernières années. Par exemple, en 2016, la Ville a signé un contrat avec un nouveau fournisseur de services de sécurité gérés dans le but d’améliorer la prestation des services et la valeur ajoutée. Nous avons aussi constaté l’examen et la mise à jour exhaustifs du cadre stratégique en matière de TI de la Ville par les STI; notamment, la nouvelle norme sur la sécurité de l’information pour les services d’accès à distance représente une grande amélioration en matière de supervision et de contrôle des solutions d’accès à distance, puisqu’elle impose des évaluations des risques. Point à noter : la vérification a conclu que des pratiques efficaces et officielles d’octroi des droits d’accès à distance étaient en place, et que les pratiques favorisant la bonne administration des comptes d’accès à distance – notamment, le rapprochement périodique des comptes des utilisateurs – avaient été améliorées.

Malgré ces améliorations, la vérification a soulevé certaines lacunes et faiblesses dans la capacité de la Ville à détecter les menaces à la sécurité et les vulnérabilités en matière d’accès à distance, et à y réagir. Plus précisément, la vérification a cerné les problèmes ci-dessous en matière de surveillance et de supervision.

- [redacted]

- Aucun test de pénétration précis n’a été mené pour des tiers connectés à partir d’un point éloigné afin de cibler les problèmes potentiels[26].

Ces problèmes sont décrits plus en détail ci-dessous.

En juin 2016, la Ville a signé un contrat avec un nouveau fournisseur de services de sécurité gérés. Durant la vérification, la Ville et son nouveau partenaire travaillaient toujours à instaurer le nouveau service. [redacted] Selon les normes de l’industrie, ce processus dure habituellement moins de trois (3) mois, soit beaucoup moins que l’expérience constatée à la Ville.

Les cas pratiques décrivent des scénarios de vulnérabilité précis que le fournisseur de services de sécurité gérés aurait à détecter dans ses activités de surveillance. Ils servent aussi de référence quant à la nature et à la portée des registres des activités et des types d’activités relatifs à l’accès à distance (ou « trafic ») que le fournisseur de services de sécurité gérés doit surveiller. Le fournisseur a instauré des cas pratiques normalisés conformément à son contrat avec la Ville. [redacted]

Dans le cadre de ses tests techniques, l’équipe de vérification a analysé les vulnérabilités des serveurs d’accès à distance de la Ville. Ces analyses n’ont pas permis de détecter des lacunes majeures, mais elles ne sont pas conçues pour offrir le même degré d’assurance qu’une analyse des vulnérabilités ciblée ou un test de pénétration menés par un tiers. On note, à l’instar des conclusions de la vérification de la gestion des incidents liés à la sécurité des TI et des interventions en la matière de 2015, qu’aucune analyse des vulnérabilités et aucun test de pénétration réguliers n’étaient menés[27] pour l’ensemble des solutions d’accès à distance de la Ville. Des

[26] Cette même observation a été faite dans la vérification de la gestion des incidents liés à la sécurité des TI et des interventions en la matière de 2015, qui recommandait que le CI mène des tests de pénétration dans toutes les infrastructures essentielles.

[27] L’équipe de vérification notait que la nouvelle solution de VPN Citrix, dont la mise en œuvre est prévue en 2017, avait fait l’objet d’une évaluation de la vulnérabilité.

entretiens avec le personnel des STI révèlent par ailleurs qu’habituellement, les STI mènent des évaluations des risques au cas par cas, selon le degré de risque perçu. La version provisoire de la norme sur la sécurité de l’information pour les services d’accès à distance (ISS-RAS) vient pallier cette lacune en exigeant que les technologies d’accès à distance fassent l’objet d’une analyse des vulnérabilités deux fois par année et d’une évaluation des risques ou des menaces au moins tous les trois ans. Comme l’indique la recommandation nº 2, le personnel est invité à mettre en œuvre cette nouvelle norme aussitôt que possible.

Selon les entretiens et les examens de documents menés durant la vérification, le rapprochement des comptes d’accès à distance[28] (ceux fournis à des employés ne travaillant pas pour la Ville) n’avait pas été réalisé dans des délais raisonnables. Cependant, au cours du processus de vérification, les STI ont commencé à vérifier leur banque de données de tiers ayant un accès à distance pour s’assurer que ces derniers avaient toujours besoin d’un accès, et que les renseignements pertinents étaient exacts et à jour (p. ex., date de fin de contrat et nom de la personne-ressource dans le secteur d’activités de la Ville). L’équipe de vérification comprend que cette amélioration dans l’administration des comptes d’accès à distance devra se traduire par des vérifications périodiques pour veiller à limiter l’accès aux comptes aux seuls utilisateurs appropriés et autorisés.

Recommandation nº 7

La Ville devrait évaluer et améliorer la gestion et la surveillance de la sécurité de l’accès à distance, en prenant notamment la mesure suivante :

- [redacted]
- Continuer d’améliorer les pratiques opérationnelles, entre autres la gestion et le rapprochement des comptes des fournisseurs et des employés.

Réponse de la direction

La direction approuve cette recommandation. [redacted] Des mesures

[28] Il s’agit de comptes de personnes qui ne travaillent pas à la Ville, notamment des entrepreneurs et fournisseurs qui, dans leurs fonctions, ont besoin d’un accès à distance.

opérationnelles seront prises afin d’améliorer la gestion des comptes des fournisseurs et de veiller au maintien des activités de rapprochement des comptes, d’ici le T4 de 2019.

Annexe A : Objectifs et critères de la vérification

Survol des objectifs et des critères de la vérification

Utilisation de l’accès à distance (politiques, procédures et normes)	
1.1	Des politiques et des procédures officielles sont établies afin : • d’obliger les utilisateurs à maintenir les contrôles de sécurité sur leurs appareils pouvant se connecter; • d’obliger les utilisateurs à respecter les politiques, les normes et les directives de la Ville; • d’obliger la tenue d’évaluations des risques dans le cadre de la sélection des méthodes d’accès à distance; • d’officialiser la gestion, l’administration et l’utilisation sécuritaires des solutions d’accès à distance.
1.2	Les normes d’accès à distance, notamment en ce qui a trait à l’authentification, au cryptage, à l’autorisation et aux types d’appareils et d’accès au réseau permis, sont officiellement définies.
Rôles et responsabilités pour octroyer le droit d’accès	
2.1	Les rôles, les responsabilités et la reddition de comptes sont clairement définis, communiqués et compris, et ce, pour toutes les parties concernées par l’accès à distance aux TI.
2.2	Les utilisateurs et les organisations capables d’utiliser l’accès à distance ont reçu une autorisation officielle avant de se voir accorder les privilèges d’accès.
2.3	Les comptes inactifs sont repérés et fermés.
Architecture et technologie d’accès à distance	
3.1	Une architecture organisationnelle d’accès à distance applicable aux systèmes de TI, au SCADA et à la technologie exclusive a été créée.
3.2	Les directions générales de la Ville ayant des besoins précis ont mis en place un système d’accès à distance adapté conforme aux politiques, aux normes et à l’architecture des STI.

3.3	Les STI consignent et évaluent la connectivité entre les systèmes d’accès à distance et le réseau de la Ville afin de détecter les risques à la sécurité.
Fonctionnement et surveillance de l’accès à distance.	
4.1	Les systèmes d’accès à distance, à l’échelle des directions générales et de la Ville, sont disponibles et fonctionnent correctement, de manière à répondre aux exigences opérationnelles établies dans un plan de continuité des activités ou une étude d’impact.
4.2	Les utilisateurs de l’accès à distance ont rapidement accès à un soutien efficace (comme les services de dépannage des TI) conforme aux normes de service.
4.3	Les correctifs et les mises à jour d’entretien sont appliqués dans des délais raisonnables, conformément aux pratiques exemplaires et aux normes de la Ville en matière de correctifs et de gestion de la vulnérabilité.
4.4	Les solutions d’accès à distance, à l’échelle des directions générales et de la Ville, ont fait l’objet d’une évaluation des risques.
4.5	Les anomalies et les brèches de sécurité dans l’infrastructure d’accès à distance sont détectées au moyen d’outils adaptés et efficaces.
4.6	Les pratiques de gestion des incidents et d’intensification de l’intervention pour l’accès à distance sont officiellement définies et suivies lors de toutes les mises en œuvre.
4.7	Les STI assurent le suivi du rendement et de la disponibilité des services d’accès à distance et avisent les intervenants concernés lorsque les attentes ne sont pas satisfaites.