Bureau de la vérificatrice générale

Suivi de la vérification de l’accès à distance aux technologies de l’information (TI) de 2017

Déposé devant le Comité de la vérification

Le 27 avril 2021

Table des matières

Résumé

La vérification de l'accès à distance aux technologies de l'information (TI) s'est déroulée en 2017 et a donné lieu à sept recommandations. Par la suite, un suivi de vérification a été inscrit dans le Plan de vérification de 2020 du Bureau du vérificateur général (BVG), afin de faire le point sur l'avancement des sept recommandations.

Voici un aperçu des recommandations :

Recommandation nº 1 : 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 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.

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.

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.

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.

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, notamment :

- en adoptant rigoureusement l'authentification bifactorielle obligatoire;
- en restreignant la capacité des utilisateurs à installer des solutions d'accès à distance non autorisées sur les terminaux confiés par la Ville.

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 :

- finaliser la mise en œuvre des cas d'utilisation propres à la surveillance des incidents de sécurité dans l'accès à distance avec leur fournisseur de services de sécurité gérés (FSSG);
- continuer d'améliorer les pratiques opérationnelles, entre autres la gestion et le rapprochement des comptes des fournisseurs et des employés.

Le suivi de la vérification de 2017 de l'accès à distance aux TI a permis d'évaluer l'état de la mise en œuvre de chaque recommandation, dont le tableau 1 ci-après donne un aperçu des résultats, ainsi que l'état déclaré par la direction au début de la vérification. Les détails de l'évaluation et les constatations détaillées sont reproduits dans la section du rapport détaillé.

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

Recommandations	**État selon la direction en août 2020**	**État selon le BVG en novembre 2020**
#1	Achevée	Achevée
#2	Achevée	Achevée
#3	Achevée	Achevée
#4	Achevée	Achevée
#5	Achevée	Achevée

Recommandations	État selon la direction en août 2020	État selon le BVG en novembre 2020
#6	Achevée	Achevée
#7	Achevée	Achevée
Total	**7 achevées (100 %)**	**7 achevées (100 %)**

Conclusion

Le suivi de la vérification de l’accès à distance aux TI a permis de constater que les sept recommandations précédentes qui découlent de la vérification de 2017 ont maintenant été mises en œuvre et sont achevées.

Puisque l’accès à distance prend encore plus d’importance pendant la pandémie de COVID-19, la Ville a adopté des mesures pour formaliser le processus correspondant et doit continuer de surveiller l’accès et de procéder à intervalles réguliers à des examens de l’évaluation des risques pour toutes les exemptions par rapport à la Norme d’accès à distance.

Remerciements

Nous tenons à remercier la direction pour la collaboration et l’assistance accordées à l’équipe de vérification.

Rapport détaillé – Avancement de la mise en œuvre

Pour procéder à l’évaluation, les vérificateurs ont examiné les documents sur les politiques et les processus essentiels de la Ville relativement à l’accès à distance aux TI, dont la Politique sur la sécurité des informations, la Norme d’accès à distance, le mandat du Comité d’examen de l’architecture, la procédure de surveillance de l’accès à distance et d’autres documents afférents.

Les vérificateurs ont aussi mené des entrevues auprès de différents membres de l’équipe de la sécurité de l’information des Services de Technologies de l’information (STI), dont le chef de l’information de la Ville, le gestionnaire de la Direction des solutions technologiques et le chef de la Sécurité de l’information et de la Gestion des risques numériques.

Le présent rapport résume l’évaluation de la direction concernant l’état d’avancement de la mise en œuvre pour chacune des recommandations en date d’août 2020, ainsi que l’évaluation du Bureau du vérificateur général (BVG) en date de novembre 2020.

Recommandation nº 1

Tableau 1 : Avancement

Mise à jour de la direction	Évaluation du BVG
Achevée	Achevée

Recommandation de la vérification

Le chef de l'information 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 initiale 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.

Mise à jour de la direction

Août 2020

Le chef de l'information s'assure que les objectifs de l'accès à l'information font partie des objectifs stratégiques des réseaux zéro-confiance et des STI dans le cadre des objectifs et résultats clés (ORC). (Voici des exemples des moyens grâce auxquels cette stratégie a été opérationnalisée pour assurer la conformité dans l'ensemble de la Ville : l'obligation de recourir à l'authentification multifactorielle dans le cadre de l'évaluation des nouvelles initiatives technologiques et la finalisation et la communication, à tous les utilisateurs de la Ville XXXX, des Normes d'accès à distance.

Évaluation du BVG

Les mesures décrites dans le compte rendu de la direction sont achevées selon l'évaluation.

Nous avons pris connaissance XXXX dans le cadre de l'assemblée générale du personnel des STI; ce diaporama précise l'approche suivie pour adopter le principe de la XXXX en ce qui a trait à l'accès aux ressources et aux systèmes de la Ville, ce qui

constitue un objectif stratégique appliqué à la Ville. La notion traditionnelle d'accès à distance serait donc analysée différemment dans un environnement XXXX, dans lequel on renonce à utiliser les réseaux privés virtuels (RPV) et un point d'accès unique. Il faut toutefois noter que l'application d'un environnement de zéro-confiance est un travail énorme, qu'il faut encore mettre en œuvre.

Nous avons constaté que l'authentification multifactorielle (AMF) est désormais une exigence est désormais une exigence du modèle de définition de la portée des travaux de février 2020 pour toutes les nouvelles demandes d'accès à Active Directory.

Le BVG a demandé d'autres pièces justificatives de l'adoption de l'AMF dans l'administration municipale. La direction a déposé un rapport sommaire, qui indique XXXX.

On a aussi noté, dans l'information fournie par la direction, que le taux d'adoption augmentera, puisque la Ville a récemment ajouté, XXXX.

Un fichier exporté de l'accès à distance en AMF XXXX a été fourni dans un tableur Excel, qui fait aussi état d'environ XXXX inscrits pour l'accès en AMF sous différentes formes, par exemple XXXX.

La direction nous a soumis les mesures d'atténuation suivantes pour les cas dans lesquels les utilisateurs pourraient ne pas faire appel à l'AMF :

- travailler activement avec le fournisseur pour paramétrer l'AMF;
- adopter la version la plus récente de [redacted] en prévision de la mise en œuvre de l'AMF;
- demander au client de se connecter d'abord au [redacted], puis d'utiliser [redacted];
- indiquer que l'AMF est obligatoire dans les nouvelles initiatives pendant le processus de prise en charge des opérations.

Recommandation nº 2

Tableau 3 : Avancement

Mise à jour de la direction	Évaluation du BVG
Achevée	Achevée

Recommandation de la vérification

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 initiale 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.

Mise à jour de la direction

Août 2020

La Norme d’accès à distance ainsi que les pratiques et les contrôles connexes ont été communiqués à tous les partenaires technologiques et à tous les employés en février et en mars 2020.

Évaluation du BVG

Nous avons examiné la Norme de sécurité technique pour les services d’accès à distance. Dans cette norme, la portée des travaux s’entend de « toutes les technologies utilisées dans la mise en œuvre, l’exploitation et la gestion des services d’accès à distance qui appuient les connexions à distance à l’environnement informatique d’entreprise de la Ville d’Ottawa. L’environnement informatique d’entreprise de la Ville comprend les environnements qui sont gérés et exploités par les partenaires fédérés et par les tiers qui archivent ou transmettent les données de la Ville ».

Cette norme est approuvée par le chef de l’information, et le contenu est contrôlé par le gestionnaire de la Direction de la sécurité technologique. Toutes les exceptions doivent être approuvées par le chef de l’information et par le directeur général ou le directeur de l’Unité opérationnelle qui souhaite se prévaloir de l’exemption.

Un exposé sur la gouvernance des solutions d’accès à distance (SAD) a été présenté aux partenaires technologiques, XXXX en février et en mars 2020.

Recommandation nº 3

Tableau 4 : Avancement

Mise à jour de la direction	Évaluation du BVG
Achevée	Achevée

Recommandation de la vérification

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 initiale 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.

Mise à jour de la direction

Août 2020

Le chef de l’information a adopté des mesures pour s’assurer que toutes les politiques étaient réactualisées et mises à jour et qu’un cycle de mise à jour sur deux ans a été mis en œuvre. Le Cadre des objectifs et résultats clés (ORC) de la Direction de la sécurité technologique prévoit un examen des politiques et des normes selon un cycle de deux ans.

Au moment d’écrire ces lignes, on était en train d’examiner et de mettre à jour deux documents des politiques sur les TI selon le cycle d’examen de deux ans (soit la Politique sur l’utilisation responsable des ordinateurs et les Normes de sécurité générale des STI). Les autres politiques qui sont du ressort des Services de technologie de l’information ont été mises à jour en 2019 et devraient être examinées en 2021.

Évaluation du BVG

Nous avons examiné le tableur XXXX et noté que parmi les huit politiques et normes énumérées, le dernier examen de cinq politiques et normes remonte à 2019 et que ces politiques et normes devraient être examinées en 2021. Toutefois, le dernier examen de la Politique sur l’utilisation responsable des ordinateurs remonte au 30 janvier 2018, et on a rédigé la version provisoire de la mise à jour de cette politique dans le cadre du Plan de travail des STI de 2020.

Nous avons noté que la Norme de sécurité technique pour les services d’accès à distance n’a pas été mise à jour depuis le 1er août 2017, soit la date à laquelle elle a été publiée; toutefois, la constatation faite à l’origine se rapporte aux politiques plutôt qu’aux normes; c’est pourquoi nous indiquons que cette recommandation est achevée.

Recommandation nº 4

Tableau 5 : Avancement

Mise à jour de la direction	Évaluation du BVG
Achevée	Achevée

Recommandation de la vérification

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 initiale 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.

Mise à jour de la direction

Août 2020

Le chef de l’information a mis en œuvre une série de fonctions et d’initiatives pour assurer la mise à jour à intervalles réguliers des diagrammes de l’architecture et pour faire évoluer la pratique générale, notamment :

1. en s’assurant qu’une architecture de référence à jour est terminée, qui comprend des normes d’infrastructure et de réseau;
2. en mettant sur pied un comité d’examen de l’architecture pour évaluer le risque technologique et les grands changements architecturaux dans toute l’infrastructure de la Ville;
3. en instituant un contrôle complet des changements pour l’ensemble de l’infrastructure, des réseaux et des terminaux dans le cadre de la Politique sur la gestion des changements et en épaulant le Conseil consultatif des changements.

Les diagrammes de l'architecture de l'accès à distance des STI et des partenaires technologiques sont consignés par écrit et sont mis à jour conformément à ces processus (travail achevé en septembre 2019).

Évaluation du BVG

Nous avons examiné le document XXXX, qui précise l'architecture technique et les systèmes utilisés à la Ville d'Ottawa. Nous avons noté que ce document n'est pas soumis à un contrôle; cependant, il porte effectivement, sur la couverture, la date de 2020, en précisant aussi qu'il s'agit d'une « demande de propositions ». Si ce document est considéré comme un texte officiel sur l'architecture de référence, il faudrait contrôler comme il se doit le document pour permettre de suivre et d'enregistrer les mises à jour et les modifications qui y sont apportées.

Nous avons examiné le document portant sur le mandat du Comité de l'examen de l'architecture (CEA) (en date du 20 novembre 2019). Nous avons constaté que le CEA se réunit toutes les deux semaines et ponctuellement selon les besoins. Le CEA est parrainé par le chef de l'information et est présidé par le chef de l'architecture de l'entreprise.

Voici les fondés de pouvoir délégués habilités à prendre les décisions voulues :

- l'architecte des opérations, l'architecte des données et de l'information, l'architecte des applications et de l'intégration, l'architecte des technologies et de l'infrastructure et l'architecte de la sécurité;
- les architectes [redacted];
- les architectes [redacted];
- [redacted] Architects;
- [redacted] Architects;
- les responsables des produits.

En outre, le mandat du CEA précise la marche à suivre quand il s'agit d'exercer des droits de vote pour prendre les décisions ou délivrer les approbations se rapportant à l'architecture.

Nous avons examiné le processus et les procédures de gestion des changements et de gestion de la configuration des STI (v2.1), dont la dernière mise à jour remonte à octobre 2019. Ce document précise la procédure de gestion des changements, dont les quatre types de demandes de changement (DC), ce qui comprend XXXX. Le Conseil consultatif sur les changements (CCC) se réunit chaque semaine, XXXX. Les DC

programmées, approuvées et achevées sont affichées dans l’échéancier prévisionnel des changements pour que les membres du CCC puissent en prendre connaissance.

Recommandation nº 5

Tableau 6 : Avancement

Mise à jour de la direction	Évaluation du BVG
Achevée	Achevée

Recommandation de la vérification

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 initiale 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.

Mise à jour de la direction

Août 2020

La base de données de gestion des configurations (BDGC) a été mise à jour afin de recenser toutes les solutions d’accès à distance (SAD). Chaque SAD correspond à un élément de configuration (EC) créé dans la BDGC, et l’EC est lié à un diagramme d’accès à distance. Il existe un processus de gestion des changements, et la formation a été donnée en décembre 2019 par tous les partenaires technologiques.

Évaluation du BVG

Nous avons examiné le tableur des EC des SAD qui reprend le contenu de la BDGC, qui dresse la liste de XXXX correspondants. Au moment de l’enquête, nous avons déposé une autre demande relativement à la consignation de la nature des droits d’accès à distance, XXXX. On nous a fourni d’autres pièces justificatives dans le tableur XXXX, le cas échéant, pour les systèmes d’accès à distance correspondants. Nous avons noté qu’il n’y a pas, pour tous les systèmes, d’EC principaux ou secondaires. Une autre amélioration consisterait à inclure les cas dans lesquels il n’est « pas pertinent » de prévoir un EC principal ou secondaire, pour que l’information soit plus claire lorsqu’il s’agit de vérifier si ces éléments de configuration ont été prévus ou omis.

Recommandation nº 6

Tableau 7 : Avancement

Mise à jour de la direction	Évaluation du BVG
Achevée	Achevée

Recommandation de la vérification

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, notamment :

- en établissant rigoureusement le principe obligatoire de l’authentification bifactorielle;
- en restreignant la capacité des utilisateurs à installer des solutions non autorisées d’accès à distance sur les terminaux confiés par la Ville.

Réponse initiale de la direction

La direction approuve cette recommandation.

Le chef de l’information mettra en œuvre les contrôles voulus pour détecter et prévenir les incidents d’accès sans autorisation et pour intervenir dans ces incidents, notamment en appliquant rigoureusement l’authentification bifactorielle pour les connexions des SAD et en surveillant et restreignant l’utilisation des solutions non autorisées d’accès à distance. Ce travail sera achevé au quatrième trimestre de 2019.

Mise à jour de la direction

Août 2020

La gestion des terminaux mobiles est en place. On a achevé le déploiement de l’authentification multifactorielle (AMF). XXXX. On traite ce cas en prévoyant une extension de la licence existante du produit. On définit XXXX et on traite les restrictions dans le cadre des opérations de la technologie de sécurité.

Évaluation du BVG

L’authentification multifactorielle a été mise en œuvre dans le cadre de la politique sur l’accès conditionnel de l’AMF pour l’accès à distance de XXXX. Nous avons pris connaissance d’un instantané d’écran de cet accès.

On nous a aussi fourni le tableur des XXXX qui fait état des risques connexes et des mesures d’atténuation pour les exemptions de la Norme des SAD. XXXX

Chaque mesure d’atténuation est confiée à un responsable des risques.

Nous avons noté que bien qu’il indique un identifiant de risque, le tableur ne comprend pas de dates pour l’examen ou la réévaluation des risques et des mesures d’atténuation correspondantes.

Recommandation nº 7

Tableau 8 : Avancement

Mise à jour de la direction	Évaluation du BVG
Achevée	Achevée

Recommandation de la vérification

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 :

- finaliser la mise en œuvre des cas d’utilisation propres à la surveillance des incidents de sécurité dans l’accès à distance avec leur FSSG;
- continuer d’améliorer les pratiques opérationnelles, entre autres la gestion et le rapprochement des comptes des fournisseurs et des employés.

Réponse initiale de la direction

La direction approuve cette recommandation.

le chef de l’information s’assurera que les cas d’utilisation propres à la surveillance des incidents de sécurité dans l’accès à distance avec les FSSG des STI sont mis en œuvre d’ici au quatrième trimestre de 2019. 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.

Mise à jour de la direction

Août 2020

La surveillance de la sécurité au sein des FSSG des STI est exercée pour les cas d’utilisation propres à l’accès à distance. La gestion des comptes et le contrôle de concordance du personnel interne et des entrepreneurs sont gérés par le Système du répertoire des entreprises (SRD) de la Ville, qui prévoit d’importantes mises à jour pour constituer ou invalider automatiquement les comptes d’après les changements de données de SAP. Ce système XXXX pour qu’ils soient synchronisés. L’AMF a aussi été mise en œuvre dans l’ensemble de l’administration municipale.

Évaluation du BVG

La direction a fait savoir que la surveillance de la sécurité est exercée XXXX.

En examinant la page 2 des Procédures administratives sur la sécurité de l’information, nous avons noté XXXX.

Relativement à la recommandation qui consiste à améliorer les pratiques opérationnelles, il y a des réunions hebdomadaires pour les Services de sécurité XXXX et des réunions hebdomadaires pour les STI XXXX. Nous avons pris connaissance du procès-verbal de la réunion sur les opérations hebdomadaires le 24 août 2020; ce procès-verbal comprend un exposé sur l’analyse à distance.

XXXX La direction nous a fourni un instantané d’écran représentant les rapports journaliers qui sont produits. En outre, on nous a fourni un cas Marval se rapportant à l’examen de XXXX.

Nous avons examiné le tableur XXXX, et nous avons noté que cette matrice indique XXXX.

Tableau 9 : Légende des degrés d’achèvement

Achèvement	Définition
À venir	Aucun progrès tangible n’a été réalisé. L’élaboration de plans non officiels n’est pas considérée comme un progrès tangible.
Partiellement achevée	La Ville a entamé la mise en œuvre, mais celle-ci n’est pas encore terminée.
Achevée	La mesure a été prise, ou les structures et les processus fonctionnent comme il se doit et ont été entièrement adoptés dans tous les secteurs concernés de la Ville.
Impossible à évaluer	Aucune mesure n’est appliquée à l’heure actuelle; toutefois, la recommandation reste applicable.