Rapport

Audit d’optimisation des ressources – Protection des renseignements personnels

Le 15 décembre 2023

Présenté à :

Raymond Chabot Grant Thornton

SAINTE-JULIE

Raymond Chabot
Grant Thornton

Raymond Chabot
Grant Thornton S.E.N.C.R.L.
Bureau 2000
Tour de la Banque Nationale
600, rue De La Gauchetière Ouest
Montréal (Québec)
H3B 4L8

T 514 878-2691

Le 15 décembre 2023

Aux membres du conseil municipal
Ville de Sainte-Julie
1580, chemin du Fer-à-Cheval
Sainte-Julie (Québec) J3E 2M1

Objet : Rapport – Audit d'optimisation des ressources – Protection des renseignements personnels

Mesdames, Messieurs,

Nous avons le plaisir de vous présenter notre rapport portant sur l'information relative à la protection des renseignements personnels par la Ville de Sainte-Julie (ci-après la « Ville »).

Ce mandat a été réalisé en vertu des dispositions de la Loi sur la Commission municipale, et le présent rapport doit être déposé à la première séance du conseil municipal qui suit sa réception par la direction de la Ville. Celui-ci doit également être publié sur le site Web de la Commission municipale du Québec.

Nous tenons à souligner l'excellente collaboration de toutes les personnes rencontrées au cours de la réalisation du mandat.

Nous vous prions de recevoir, Mesdames, Messieurs, nos salutations les plus distinguées.

Raymond Chabot Grant Thornton S.E.N.C.R.L.[1]

[1] CPA auditeur, permis de comptabilité publique nº A129112

Table des matières

1. Contexte et objectifs

1.1. CONTEXTE

La Ville de Sainte-Julie (ci-après la « Ville ») collecte et traite des renseignements personnels (« RP ») afférents à la vie privée de ses employés et des citoyens. La Ville compte plus de 30 000 citoyens et plus de 240 employés. Les informations détenues par la Ville sont nécessaires afin de servir adéquatement les citoyens et consistent en des :

- dossiers d'employés, leurs dossiers médicaux ainsi que leurs coordonnées bancaires;
- candidatures aux fins de recrutement;
- informations personnelles des citoyens pour l'utilisation des services en ligne, comme les demandes de permis, le paiement de stationnement et la taxation.

La Ville étant un organisme municipal, elle est assujettie à la loi pour le secteur public : Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. Cette loi s'applique à tous les documents, peu importe leur format : écrit, graphique, sonore, visuel, informatisé ou autre.

De plus, la Ville est également assujettie à la nouvelle Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (ci-après la « loi 25 »), dont certaines dispositions sont entrées en vigueur le 22 septembre 2022 et d'autres dispositions entreront progressivement en vigueur jusqu'en 2024. Les nouvelles obligations relatives à cette loi exigent, entre autres[1] :

- de désigner une personne responsable de la protection des renseignements personnels et de publier son titre et ses coordonnées sur le site Internet de la Ville;
- de tenir un registre de tous les incidents de confidentialité, de prendre rapidement des mesures afin de diminuer le risque qu'un préjudice soit causé aux personnes concernées et d'aviser la Commission d'accès à l'information du Québec pour les incidents présentant un risque sérieux de préjudice;
- de former un comité sur l'accès à l'information et la protection des renseignements personnels;
- de mettre en œuvre des politiques et des pratiques encadrant la gouvernance des renseignements personnels;
- de publier une politique de confidentialité si des renseignements personnels sont recueillis par un moyen technologique;

[1] : Extrait de l'aide-mémoire : Résumé des nouvelles obligations des entreprises – Commission d'accès à l'information du Québec.

- de respecter les nouvelles règles de consentement définies;
- de détruire les renseignements personnels lorsque la finalité de leur collecte est accomplie, ou les anonymiser pour les utiliser à des fins sérieuses et légitimes, sous réserve des conditions et d'un délai de conservation prévus par une loi;
- de respecter les nouvelles règles d'utilisation des renseignements personnels;
- de prévoir, par défaut, les paramètres assurant le plus haut niveau de confidentialité du produit ou du service technologique offert au public;
- etc.

Les renseignements personnels sont définis par les RP, qui portent sur une personne physique et permettent de l'identifier. Ils sont confidentiels. Sauf exception, ils ne peuvent être communiqués sans le consentement de la personne concernée.

Des exemples de RP :

- Nom, prénom, pseudonyme, date de naissance, NAS;
- Photos, enregistrements sonores de voix;
- Numéro de téléphone fixe ou portable, adresse postale, adresse courriel;
- Adresse IP, identifiant de connexion informatique ou identifiant de *cookie*;
- Numéro de plaque d'immatriculation, numéro d'une pièce d'identité, coordonnées bancaires;
- Données relatives à la santé des individus;
- Données concernant la vie sexuelle ou l'orientation sexuelle;
- Données qui révèlent une prétendue origine raciale ou ethnique.

Certaines données sont de nature publique, comme le rôle d'évaluation et de taxation, où l'on retrouve les informations des propriétaires, soit le nom, le prénom, l'adresse et le rôle d'évaluation du terrain et du bâtiment.

Les conséquences d'une mauvaise protection des RP, en plus de ne pas être conformes à la loi, peuvent être de permettre la divulgation non autorisée des RP, qu'une personne mal intentionnée utilise l'information des RP aux fins d'usurpation d'identité, d'atteinte à la réputation de la Ville ou de perte de confiance des citoyens envers la Ville ainsi que des poursuites judiciaires.

2. Objectif de l’audit et portée des travaux

2.1. OBJECTIF DE L’AUDIT

Nous avons réalisé une mission d’audit de l’optimisation des ressources portant sur la protection des renseignements personnels.

Cet audit avait pour objectif de s’assurer que les renseignements personnels détenus par la Ville faisaient l’objet d’une protection adéquate afin de mitiger les risques de bris de confidentialité, de vol ou d’accès non autorisés aux RP.

Responsabilité de la direction

La direction de la Ville est responsable de la protection des renseignements personnels qu’elle détient. Elle est également responsable de la mise en place des systèmes, des procédures et des contrôles lui permettant d’identifier, de gérer et de protéger les renseignements personnels, et ce, conformément aux règles en vigueur et aux saines pratiques en matière de protection des renseignements personnels.

Responsabilité de l’auditeur

Notre responsabilité consiste à fournir une conclusion sur les objectifs de l’audit. Pour ce faire, nous estimons que nous avons recueilli les éléments probants suffisants et appropriés pour fonder notre conclusion et pour obtenir un niveau d’assurance raisonnable. Notre évaluation est basée sur les critères que nous avons jugés valables dans les circonstances. Ces derniers sont exposés à la section 5.2.

Nous avons planifié et réalisé notre mission d’assurance raisonnable conformément à la norme canadienne de missions de certification (NCMC) 3001, Missions d’appréciation directe, du *Manuel de CPA Canada – Certification.* Cette norme requiert que nous planifiions et réalisions la mission de façon à obtenir une assurance raisonnable à l’égard de notre conclusion sur l’objectif de l’audit.

L’assurance raisonnable correspond à un niveau élevé d’assurance, qui ne garantit toutefois pas qu’une mission réalisée conformément à cette norme permettra toujours de détecter tout cas important de non-conformité ou les déficiences significatives qui pourraient exister. Les cas de non-conformité ou déficiences significatives aux critères peuvent résulter de fraudes ou d’erreurs et ils sont considérés comme significatifs lorsqu’il est raisonnable de s’attendre à ce que, individuellement ou collectivement, ils puissent influer sur les décisions des utilisateurs de notre rapport. Une mission d’assurance raisonnable visant la délivrance d’un rapport de l’auditeur implique la mise en œuvre de procédures en vue d’obtenir des éléments probants suffisants et appropriés pour fonder raisonnablement une conclusion et obtenir un niveau d’assurance élevé. La nature, le calendrier et l’étendue des procédures d’audit choisies relèvent de notre jugement professionnel, et notamment de notre évaluation des risques de non-conformité ou de déficiences significatives, que celles-ci résultent de fraudes ou d’erreurs.

Notre indépendance et notre gestion de la qualité

Nous nous sommes conformés aux règles ou au code de déontologie pertinents applicables à l'exercice de l'expertise comptable et se rapportant aux missions de certification, qui sont publiés par les différents organismes professionnels comptables, lesquels reposent sur les principes fondamentaux d'intégrité, d'objectivité, de compétence professionnelle et de diligence, de confidentialité et de conduite professionnelle.

Notre cabinet applique la norme canadienne de gestion de la qualité (NCGQ) 1, *Gestion de la qualité par les cabinets qui réalisent des audits ou des examens d'états financiers, ou d'autres missions de certification ou de services connexes*. Cette norme exige du cabinet qu'il conçoive, mette en place et fasse fonctionner un système de gestion de la qualité qui comprend des politiques et des procédures en ce qui concerne la conformité aux règles de déontologie, aux normes professionnelles et aux exigences légales et réglementaires applicables.

2.2. PORTÉE DES TRAVAUX

Nos travaux d'audit ont porté sur la période du 15 mai 2023 au 15 juillet 2023. Nous avons toutefois tenu compte d'informations qui nous ont été transmises jusqu'en novembre 2023.

Nos travaux se sont limités et ont été réalisés sur un échantillon de systèmes contenant des RP jugés critiques par la Ville. Les systèmes sélectionnés sont les suivants :

- Coba : système de paie (hébergé par la Ville);
- Sport-Plus : système de gestion des loisirs (« SAAS ») (géré et hébergé par un fournisseur externe);
- Symphonie : système d'inscription à la bibliothèque (hébergé par la Ville);
- Serveur de fichiers et contrôleur de domaine : système gérant les fichiers et les utilisateurs sur le réseau (hébergé par la Ville).

Bien qu'il s'agisse d'un audit, notre mission ne constitue pas en soi un exercice de conformité à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, à la loi 25, ni aux autres lois et normes auxquelles la Ville pourrait se référer en ce qui concerne les RP.

À la fin de nos travaux, un rapport préliminaire comprenant nos constats a été présenté aux instances concernées de la Ville, et ce, aux fins de discussion. Par la suite, le rapport final a été transmis aux mêmes instances pour l'obtention d'un plan d'action et d'un échéancier pour la mise en œuvre des recommandations les concernant.

3. Résultats de l'audit

3.1. GOUVERNANCE

La gouvernance est un élément important pour la Ville, car elle vient établir et officialiser les orientations prises par la direction et le conseil municipal. Elle jette les bases des attentes de la Ville envers ses employés, les consultants ainsi que les fournisseurs avec qui elle collabore. Une bonne gouvernance permet de venir encadrer les principes et les standards souhaités par la Ville et cette notion s'applique à l'ensemble des sphères d'une ville, incluant le respect des renseignements personnels.

Plus précisément, la gouvernance à l'égard des technologies de l'information (TI) s'entend de la gestion et du contrôle de l'environnement TI, notamment les données utiles à une organisation et à ses parties prenantes. La gouvernance des TI exige un leadership, des structures organisationnelles, des politiques, des processus et des contrôles internes afin que les TI respectent la stratégie et les objectifs de la Ville et de ses parties prenantes. Elle englobe les efforts des employés et les processus qui soutiennent la prise de décisions relatives aux initiatives technologiques. Lorsqu'elle est mise en œuvre avec efficacité, cette gouvernance permet d'atteindre un équilibre entre la création de valeur et l'atténuation des risques pour la Ville.

3.1.1. Politiques

La mise en place de politiques des TI permet de venir encadrer la gouvernance. Celles-ci établissent les attentes et les comportements attendus en matière de sécurité de l'information et de protection des renseignements personnels.

Ces politiques doivent être formellement autorisées par la direction, revues périodiquement et diffusées à l'ensemble des employés, consultants et fournisseurs.

Dans le cadre de notre audit, nous avons observé l'existence des politiques « Internet et services en ligne » et « Utilisation du téléphone cellulaire », élaborées en 2016 et en 2017. La politique « Internet et services en ligne » décrit ce que l'employé est autorisé ou non autorisé à faire avec les accès Internet et les services en ligne. La politique sur le cellulaire confirme les règles d'utilisation des cellulaires fournis par la Ville. Cependant, il n'y a pas de politique de sécurité de l'information définissant les objectifs et les mécanismes de sécurité de l'information en place.

Nous avons également noté que la Ville a mis en place en septembre 2023 une politique de confidentialité de l'information pour les citoyens, ainsi que la politique-cadre sur la gouvernance de la protection des RP qui vient établir la gouvernance et qui décrit les lignes directrices sur la protection des RP au sein de la Ville. Cependant, il n'y a pas de politique de confidentialité et de gestion des témoins (*cookies*) disponible sur le site Web, à l'exception de la portion SAAS gérée de Sport-Plus, où une politique de gestion des témoins est disponible.

Recommandations

- Nous recommandons à la Ville d'élaborer une politique à l'égard de la sécurité de l'information, celle-ci définissant les objectifs et les mécanismes de sécurité de l'information au sein de la Ville. Cette politique pourra intégrer les concepts abordés aux politiques « Internet et services en ligne » et « Utilisation du téléphone cellulaire ».
- Nous recommandons à la Ville d'élaborer une politique de confidentialité et de gestion des témoins (*cookies*).
- Nous recommandons à la Ville que les politiques soient diffusées à l'ensemble des employés, consultants et fournisseurs, lorsqu'applicables. Les nouveaux employés devront en prendre connaissance à leur arrivée et tous les employés devront prendre connaissance de celles-ci lorsque des changements importants seront apportés aux politiques. Celles-ci devront être révisées périodiquement.

3.1.2. Comités et responsables des RP

La mise en place de comités permet de suivre l'application des politiques et procédure, et de s'assurer que les attentes sont bien gérées. Les comités doivent se rencontrer périodiquement et tenir des minutes des résolutions prises ou des actions à prendre.

Un responsable de la protection des renseignements personnels (RPRP) doit avoir été mandaté formellement par la Ville et les coordonnées de celui-ci doivent être affichées, sur le site Web de la Ville, afin de se conformer aux exigences de la loi.

Nous avons observé la mise en place d'un comité sur l'accès à l'information et la protection des renseignements personnels, celui-ci étant composé du directeur général adjoint et trésorier, de la greffière, de la greffière adjointe, du chef de section des technologies et du technicien aux archives. Les rôles et responsabilités de ce comité sont définis dans la politique-cadre sur la gouvernance des RP.

La Ville a également mandaté la greffière adjointe à titre de RPRP lors d'une séance du conseil municipal d'août 2022. Une personne substitut a également été nommée en cas d'absence de la greffière adjointe. De plus, les coordonnées pour contacter le RPRP sont disponibles sur le site Web de la Ville.

3.1.3. Classification et inventaire des renseignements personnels

Les organismes publics se doivent d'établir et de maintenir à jour un inventaire de leurs fichiers contenant des renseignements personnels. Cela est requis par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. L'article 76 de cette loi indique ce que doit contenir l'inventaire :

- La désignation de chaque fichier, les catégories de renseignements qu'il contient, les fins pour lesquelles les renseignements sont conservés et le mode de gestion de chaque fichier;
- La provenance des renseignements versés à chaque fichier;
- Les catégories de personnes concernées par les renseignements versés à chaque fichier;
- Les catégories de personnes qui ont accès à chaque fichier dans l'exercice de leurs fonctions;
- Les mesures de sécurité prises pour assurer la protection des renseignements personnels.

Une classification et un inventaire des RP permettent de mieux maîtriser les actifs informationnels de l'organisation pour ainsi déployer les mesures nécessaires pour la protection de ceux-ci. Cela permet de bien déterminer les objectifs en matière de sécurité de l'information et de protection des RP.

De plus, les organismes publics doivent avoir mis en place les mécanismes nécessaires permettant de répondre à une demande d'un citoyen ou d'un employé en ce qui concerne les renseignements personnels collectés, traités et conservés, incluant les fins pour lesquelles les données sont conservées, et ce, dans les délais prescrits.

Dans le cadre de notre audit, nous avons noté que bien que la Ville dispose d'un inventaire des actifs informationnels, celui-ci ne détaille pas l'inventaire des systèmes ni les informations sur les RP qu'ils contiennent. De plus, les documents papier conservés et les RP qu'ils contiennent ne sont pas inventoriés.

Nous avons également noté que la Ville n'a pas mis en place les mécanismes permettant de répondre à une demande d'un citoyen ou d'un employé.

Recommandations

- Nous recommandons à la Ville de mettre à jour son inventaire des actifs en y incluant les RP, et ce, autant pour les documents papier que pour les données électroniques. Cet inventaire devra être maintenu à jour afin de se conformer à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et afin de permettre à la Ville d'identifier les renseignements personnels détenus par la Ville, et ce, autant sur support papier qu'électronique.
- Nous recommandons à la Ville de communiquer l'inventaire des actifs informationnels et les attentes auprès de la direction des différents services afin qu'elle soit impliquée dans le maintien de l'inventaire et la classification des renseignements, incluant les RP.
- Nous recommandons à la Ville de mettre en place les mécanismes nécessaires pour permettre aux citoyens et aux employés de faire des demandes concernant les RP collectés, traités et conservés et que la Ville puisse répondre à ces demandes dans les délais prescrits.

3.1.4. Programme de sensibilisation

La sensibilisation à la sécurité des TI est indispensable afin de protéger une organisation de personnes malveillantes et afin de prévenir les cyberattaques potentielles. En effet, les techniques utilisées sont de plus en plus sophistiquées et les employés, consultants et fournisseurs sont souvent les premiers visés par ces cyberattaques, et ce, de par leur manque de connaissances au sujet de celles-ci.

Ceux-ci ont donc tous un rôle important à jouer à l'égard de la sécurité de l'information. Il est primordial de mettre en place un programme de sensibilisation. Un tel programme permet de transmettre aux utilisateurs les connaissances nécessaires afin de protéger l'organisation et ses RP. Un programme de sensibilisation performant contient des formations sur la sécurité des TI et sur la protection des RP, des simulations d'hameçonnage et d'autres exercices afin d'informer les utilisateurs des façons pour se prémunir de menaces comme l'hameçonnage, le harponnage, les rançongiciels, l'ingénierie sociale, etc.

Nous avons constaté la mise en place d'un programme de sensibilisation auprès des employés par l'entremise d'une firme externe qui offre un outil permettant de :

- mener des campagnes mensuelles de sensibilisation;
- mener des campagnes mensuelles de simulations d'hameçonnage;
- produire des bulletins d'information mensuels.

L'outil utilisé permet de faire le suivi des employés n'ayant pas assisté aux formations et de les relancer pour que tous les employés puissent suivre les formations. Cependant, il n'y a pas eu de campagne de sensibilisation formelle ou de formation sur la sécurité de l'information et des RP auprès de l'ensemble des employés de la Ville.

Recommandation

- Nous recommandons à la Ville de mettre à jour son programme de sensibilisation à l'égard de la sécurité de l'information et de la protection des RP. Le programme devrait être revu annuellement et diffusé auprès de l'ensemble des employés et consultants de la Ville, lorsqu'applicable. Un tel programme peut prendre diverses formes, telles que des courriels de rappel de sécurité, de la formation continue sur des sujets d'actualité ainsi que des simulations et exercices afin de tester le niveau de connaissances et de conscience en matière de sécurité.

3.2. CONSERVATION ET DESTRUCTION DES RP

La Ville doit prendre les mesures de sécurité nécessaires afin d'assurer la protection des RP collectés, utilisés, communiqués, conservés ou détruits, comme l'exige la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels ainsi que la loi 25.

Une organisation doit s'assurer de définir des règles et procédures à l'égard de la conservation et de la destruction des données, dont les RP, et ce, autant en ce qui concerne les données sur support papier et support électronique. En effet, la capacité et le désir de conserver d'importantes quantités de renseignements personnels augmentent les risques relatifs à la protection des renseignements personnels. De ce fait, les durées de conservation doivent être clairement établies et tenir compte des exigences réglementaires applicables et de l'objectif initial ayant mené à la collecte de ces données.

En ce qui concerne la destruction de ces données lorsque la durée de conservation a été atteinte, une organisation doit définir les procédures visant à détruire irrémédiablement le support sur lequel sont stockées ces données, de sorte qu'il soit impossible de reconstituer celles-ci de quelque façon que ce soit. De plus, ces procédures doivent également tenir compte de la destruction de toutes les copies ainsi que de tous les fichiers de sauvegarde.

Dans le cadre de notre audit, nous avons pris en considération les RP conservés ou détruits. Pour conserver et par la suite détruire les RP au bon moment, un calendrier de conservation doit être instauré. La Ville a un plan de classification qui contient le recueil des délais de conservation des données, dont les RP. Le calendrier a été élaboré selon les règles de la BAnQ (Bibliothèque et Archives nationales du Québec). Le calendrier de conservation est en place avec une durée de vie attribuée selon la nature du document et lorsque celle-ci est atteinte, les documents (supports papier

ou électronique) sont archivés, conservés ou détruits. Cependant, ce calendrier ne peut être efficace qu'avec la mise en place et le maintien d'un inventaire des actifs informationnels, incluant les RP.

L'accès à la salle des archives est restreint par une porte verrouillée à clé. Cependant, nous avons noté qu'il n'y a pas de registre des personnes détenant une clé permettant d'accéder aux archives et la clé maître est disponible à proximité. Une gestion des accès par l'entremise d'une clé est plus complexe qu'une gestion des accès par l'entremise de cartes d'accès magnétiques, celles-ci facilitant la gestion des accès et permettant une imputabilité des actions.

En ce qui concerne la conservation des données électroniques, la Ville réalise la sauvegarde informatique de ses serveurs, dont le serveur de fichiers. Cette sauvegarde est effectuée directement dans la salle secondaire, à partir de laquelle deux copies sont réalisées, l'une déposée dans l'infonuagique à l'extérieur du réseau de la Ville et la seconde dans un autre site secondaire. Les sauvegardes sont chiffrées, permettant de s'assurer que les données ne sont lisibles que par le personnel autorisé.

Concernant la destruction des archives, cela se fait via une entreprise spécialisée lorsque de grandes quantités sont à détruire, sinon cela se fait à l'interne avec des déchiqueteuses à lames croisées. Les archives sont détruites au terme de leur délai de conservation. Concernant les données électroniques, les disques durs ou autres équipements qui doivent être détruits sont remis à une compagnie spécialisée dans la destruction d'équipements électroniques qui émet un certificat d'effacement des données.

Finalement, pour les données gérées par les tiers, les contrats ne spécifient pas les obligations quant à la conservation et à la destruction des données.

Recommandations

- Nous recommandons à la Ville de mettre en place un processus formel afin de gérer les accès aux divers sites d'archives et de restreindre l'accès au personnel approprié uniquement.
- Nous recommandons à la Ville d'inclure, dans les contrats avec les fournisseurs hébergeant des RP, des clauses sur les durées de conservation et la destruction des données, et ce, en ligne avec le plan de classification de la Ville.

3.3. MESURES DE PROTECTION

Comme indiqué précédemment et selon l'article 63.1 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, l'organisme public doit prendre les mesures propres à assurer la protection des RP. Les mesures de protection sont les procédures et contrôles mis en place par la Ville afin de protéger l'accès non autorisé aux RP. Nous avons évalué les procédures et contrôles en lien avec les activités suivantes :

- Gestion des accès logiques et physiques;
- Gestion des vulnérabilités;
- Gestion des incidents et de la surveillance;
- Gestion des fournisseurs.

3.3.1. Gestion des accès logiques et physiques

Accès logiques

La gestion des accès logiques vise à assurer que les accès aux systèmes contenant des RP ou aux RP directement sont restreints au personnel approprié en fonction de ses rôles et responsabilités. La mise en place de contrôles d'accès vise à :

- gérer et contrôler les accès logiques aux systèmes et aux données;
- détecter des accès non autorisés;
- définir les règles en matière d'identification, d'authentification et d'autorisation d'accès.

Nous avons évalué les mesures en place afin de contrôler et de restreindre l'accès aux RP pour les systèmes inclus dans la portée de nos travaux, soit les systèmes Coba, Sport-Plus, Symphonie, ainsi que le serveur de fichiers et le contrôleur de domaine.

Gestion des octrois, modifications et retraits d'accès

La mise en place de mesures de contrôle relatives à l'octroi, à la modification et au retrait d'accès vise à assurer que les accès octroyés à un employé sont formellement autorisés et restreints en fonction des rôles et responsabilités de celui-ci. De plus, ces mesures visent à assurer que lors du départ d'un employé ou lors d'un changement de fonction, les accès de l'employé sont retirés ou modifiés, et ce, en temps opportun.

Octroi et modification des accès

Un formulaire de demande d'accès est en place, mais n'est pas toujours utilisé lors d'une requête d'accès. De plus, bien que le formulaire contienne une section d'approbation pour la remise du matériel informatique, il n'y a pas d'approbation requise au niveau des accès à octroyer dans les différentes applications et sur le réseau.

Les accès aux applications sont gérés par une ou des personnes du service responsable de l'application (désigné comme responsable des accès à l'application). Le processus de gestion des accès à la Ville est généralement informel et non documenté. Les responsables des applications vont eux-mêmes octroyer les rôles et fonctions de chaque employé. De plus, il n'y a pas de propriétaire de données qui procède à l'approbation des demandes.

Retrait des accès

Nous avons noté que le processus de retrait des accès n'est pas formalisé. Le service des TI est informé par le service des ressources humaines du départ d'un employé, et celui-ci procède au retrait des accès au réseau de l'employé en question. Cependant, le service des TI ne reçoit pas toujours l'information du service des ressources humaines.

Le même constat est applicable au niveau des applications, les responsables de celles-ci n'étant pas toujours avisés des départs, ce qui augmente le risque que les accès ne soient pas retirés en temps opportun.

Comptes génériques à hauts privilèges

Un compte générique est un compte n'appartenant pas à un utilisateur en particulier et pouvant être utilisé par plusieurs utilisateurs. Un tel compte comporte généralement des accès privilégiés et ne permet pas l'imputabilité des actions commises. Dans le contexte des RP, il peut aussi y avoir des comptes génériques avec de moindres privilèges, mais possédant des accès en lecture ou écritures aux RP. Cela peut rendre difficile l'imputation des actions ou des accès aux RP en cas de bris de confidentialité avec ces comptes génériques.

Dans le cadre de notre audit, nous avons relevé l'existence de comptes génériques au contrôleur de domaine, Coba – paie et Symphonie, ceux-ci étant utilisés et partagés par des membres du service des TI, des membres du service responsable ou directement par le fournisseur de l'application. De plus, il est à noter qu'il n'y a pas de contrôles en place concernant les comptes à privilèges des fournisseurs des applications dans l'étendue d'audit.

Finalement, nous avons noté l'existence d'un compte générique à hauts privilèges dans Coba – paie pour lequel la Ville n'a pas été en mesure de déterminer si le compte était utilisé et dans l'affirmative, par qui.

Gestion des rôles des utilisateurs

Une bonne pratique dans la gestion des droits d'accès est d'utiliser des groupes bien définis et d'octroyer aux utilisateurs des groupes spécifiques en fonction de leurs responsabilités. Ce processus de gestion par groupe permet de plus facilement gérer les accès, autant lors de l'octroi que lors d'une modification ou d'une révision des accès. Les accès sont gérés par groupe pour les applications et pour le réseau, sauf pour l'application Sport-Plus. En effet, les accès sont octroyés à la pièce et non par groupe. De plus, il n'est pas possible de sortir une liste des utilisateurs et de leurs accès à partir de l'application, rendant difficile l'exercice de validation de la séparation de tâches et des accès aux RP.

Accès aux bases de données

Les accès aux bases de données sont réservés au service des TI ou aux fournisseurs selon les applications auditées.

Recommandations

- Nous recommandons à la Ville de formaliser le processus d'octroi et de modification des accès pour les applications et les serveurs de fichiers. Le processus doit comprendre une autorisation du propriétaire des données avant d'octroyer un accès. Ce processus doit être documenté et appliqué à toutes les applications, aussi bien au niveau du réseau que des répertoires de fichiers confidentiels.
- Nous recommandons à la Ville de restreindre au service des TI la capacité de gérer les accès aux applications, et ce, afin d'assurer une séparation adéquate des tâches.
- Nous recommandons à la Ville de mettre en place un processus formel afin d'aviser le service des TI et de retirer les accès en temps opportun lors du départ d'un employé. Le processus pourrait être automatisé, par l'entremise du logiciel Coba, ou manuellement.

- Nous recommandons à la Ville d'éviter l'utilisation de comptes génériques afin d'assurer l'imputabilité des actions commises. Dans les situations où l'utilisation de tels comptes est nécessaire, la Ville devra mettre en place des mesures afin d'assurer l'imputabilité des actions, comme l'instauration d'une voûte de mots de passe qui permet de journaliser les accès aux mots de passe et le moment de l'utilisation par un utilisateur.
- Nous recommandons à la Ville, pour l'application Sport-Plus, d'entreprendre des démarches auprès du fournisseur sur la possibilité de gérer les accès par profil et non à la pièce ainsi que de permettre l'extraction d'une liste des utilisateurs et de leurs accès aux fins de révision.
- Nous recommandons à la Ville de surveiller les comptes génériques attribués aux fournisseurs afin de s'assurer que leur utilisation est restreinte et autorisée. Ces accès peuvent également être octroyés, au besoin seulement, pour limiter un accès permanent aux environnements de la Ville.

Révision périodique des accès

Une révision périodique des accès permet au responsable d'un système de confirmer que seuls les accès autorisés sont effectifs, que les accès sont conformes aux rôles et responsabilités des utilisateurs et que les accès aux RP sont restreints au personnel approprié.

Nous avons noté qu'il n'y a présentement pas de processus défini à la Ville en ce qui concerne la révision périodique des accès. Il n'y a aucune révision des accès aux applications, incluant la juste séparation des tâches et l'accès aux RP, en lecture ou en écriture, de leurs bases de données et des systèmes de fichiers et du contrôleur de domaine. De plus, comme mentionné précédemment, l'application Sport-Plus ne permet pas d'extraire une liste des utilisateurs et de leurs accès, rendant le processus de révision des accès très laborieux, et ne permet pas d'avoir une vue globale des accès aux RP.

Cependant, il est à noter que certaines applications comme Coba – paie ainsi que les bases de données n'ont pas beaucoup d'utilisateurs, limitant ainsi le risque d'accès non autorisés.

Recommandation

- Nous recommandons à la Ville de mettre en place un processus formel de révision périodique des accès. Ce processus doit comprendre la revue complète des utilisateurs et de leurs rôles pour s'assurer de la juste séparation des tâches ainsi que l'accès aux RP, autant en lecture qu'en écriture, est restreint au personnel approprié. Le processus devrait être appliqué pour l'ensemble des applications ainsi qu'aux accès aux serveurs de fichiers contenant des RP.

  En ce qui concerne les accès aux bases de données et aux systèmes d'exploitation, cette révision devrait être effectuée par la direction du service des TI.

Authentification et gestion des mots de passe

L'authentification, soit la combinaison d'un code d'utilisateur et d'un mot de passe, doit être assez robuste afin de limiter les risques d'accès non autorisés. Dans le cadre de nos travaux, nous avons évalué les paramètres de mots de passe des systèmes dans notre portée. À cet effet, nous avons noté que les paramètres de mots de passe pour certaines applications dans l'étendue de nos travaux et le réseau n'étaient pas conformes aux bonnes pratiques en ce qui concerne l'expiration, la longueur minimale, la complexité des mots de passe et/ou le verrouillage après un nombre de tentatives erronées.

Recommandations

- Nous recommandons à la Ville d'établir une politique de mots de passe alignée aux bonnes pratiques en matière d'authentification, et de veiller à son implémentation sur le contrôleur de domaine, ainsi qu'à l'ensemble des applications.

  La Ville devrait également envisager de poursuivre la mise en place d'une authentification multifacteurs de ses applications critiques afin de renforcer le processus d'authentification, et ce, en complément de la mise en place de paramètres de mots de passe plus robustes.

Accès physiques

La gestion des accès physiques vise à assurer que les accès aux salles des serveurs hébergeant les systèmes contenant des RP sont restreints au personnel approprié en fonction de leurs rôles et responsabilités. Il est à noter que la gestion des accès aux salles d'archives a été adressée à la section 3.2 – Conservation et destruction des RP.

En ce qui concerne les salles des serveurs, le principe est le même que pour les salles d'archives, l'accès aux salles étant protégé par une porte verrouillée par un code, celui-ci n'ayant pas été changé depuis plusieurs années. Le mécanisme de verrouillage par code ne permet pas d'identifier les personnes ayant accédé à la salle ni de journaliser quand elle a été accédée. De plus, il n'y a pas de caméra aux entrées des salles des serveurs permettant de surveiller les entrées et sorties.

Dans une situation où de l'équipement contenant des RP est volé où en cas d'accès non autorisé aux serveurs, il serait difficile, voire impossible, de déterminer qui a accédé aux salles.

Recommandation

- Nous recommandons à la Ville de mettre en place des mécanismes visant à restreindre l'accès aux salles des serveurs et assurant l'imputabilité et la traçabilité des accès.

3.3.2. Gestion des vulnérabilités

La gestion des vulnérabilités est un processus qui vise la découverte proactive de menaces, la surveillance en continu des actifs informationnels d'une organisation ainsi que la mise en place de mesures afin de prévenir et de détecter les menaces, incluant celles reliées aux RP.

La gestion des vulnérabilités comprend la mise en place de contrôles relatifs à l'évaluation des vulnérabilités de sécurité, la mise à jour des rustines (*patches*) sur les serveurs et les applications, la mise en place d'antivirus et l'exécution de tests d'intrusion.

Mise à jour des rustines (*patches*)

Nous avons évalué le processus de mise à jour des serveurs et des applications dans la portée de nos travaux. L'équipe du service des TI a configuré des tâches récurrentes dans le système de billetterie pour faire les mises à jour des serveurs régulièrement. Les postes de travail des employés sont quant à eux mis à jour automatiquement. Lors de notre audit, nous avons constaté que les serveurs étaient à jour et que les rustines de sécurité étaient installées.

Antivirus

Les postes de travail et les serveurs sont tous protégés par un antivirus qui se met à jour automatiquement. Il s'agit d'un service offert par un fournisseur qui fait le suivi des alertes et avise la Ville en cas de problématique. Les utilisateurs ne sont pas en mesure de désactiver l'antivirus sur leur poste de travail.

Coupe-feu

Nous avons observé l'existence de coupe-feux aux différents points d'entrée du réseau de la Ville qui sont munis d'un IPS (*Intrusion Prevention System*). Les coupe-feux sont maintenus à jour et les règles sont révisées, et ce, au besoin. Nous avons noté qu'il y a différentes zones réseau qui permettent de protéger les données, comme les RP. Aussi, nous avons observé un diagramme réseau qui permet de visualiser la façon dont les divers équipements communiquent entre eux.

Tests d'intrusion

Nous avons noté qu'il n'y a pas eu de tests d'intrusion sur les réseaux interne et externe réalisés par une firme externe. Les tests d'intrusion permettent à la Ville de valider si ses réseaux comportent des failles de sécurité qu'une personne malintentionnée pourrait utiliser. Les vulnérabilités soulevées lors de tels tests doivent être suivies et corrigées en fonction de leur importance.

Recommandation

- Nous recommandons à la Ville de réaliser annuellement des tests d'intrusion sur les réseaux externe et interne, et ce, par l'entremise d'une firme de sécurité externe. Les vulnérabilités à corriger doivent être suivies et priorisées en fonction de leur criticité.

3.3.3. Gestion des incidents et de la surveillance

Un processus de gestion des incidents vise à identifier les incidents de sécurité, incluant les incidents afférents aux RP, et permet de s'assurer que des mesures de mitigation appropriées sont mises en place afin d'éviter qu'un incident se reproduise.

La gestion des incidents de sécurité se fait par le service des TI de la Ville, mais le processus est informel. Comme cela n'est pas documenté, il n'est donc pas possible d'avoir une vue globale des incidents et des problèmes, ce qui permettrait d'identifier les tendances ou les incidents récurrents.

De plus, il n'y a pas de processus formel de détection et d'escalade en cas d'incident de sécurité et de bris de RP. Un tel processus permet d'être prêt à l'éventualité d'un incident de sécurité ou de bris de RP, d'être en mesure de répondre rapidement lors de l'incident et d'encadrer les différentes étapes à réaliser afin de résoudre l'incident dans les meilleurs délais.

Les journaux (*logs*) de l'infrastructure du réseau ne sont pas analysés périodiquement par le service des TI. L'équipe des TI fera des validations seulement en cas de problématique et non de manière proactive et préventive. L'analyse des journaux ou l'utilisation d'un système d'analyse des journaux permet de détecter rapidement si une intrusion ou des actions malveillantes surviennent sur le réseau.

Finalement, nous avons noté qu'il n'y a pas de plan de relève TI formellement documenté. Un plan de relève TI permet d'être en mesure de réagir rapidement en cas d'incident majeur ou de désastre, et permet de définir les applications critiques à relever en premier.

Recommandations

- Nous recommandons à la Ville de mettre en place un processus formel relatif à la documentation des incidents de sécurité. La documentation doit comprendre, entre autres, une chronologie des événements, une description sommaire des événements, les actifs impactés, incluant si des RP sont touchés, le plan d'action pour résoudre l'incident, etc.
- Nous recommandons à la Ville d'élaborer un processus de gestion des incidents portant atteinte à la confidentialité des RP, incluant notamment le rôle du RPRP, le processus de remontée des incidents, l'identification des incidents, la méthodologie afin d'évaluer les incidents, le délai de notification à la Commission d'accès à l'information, le processus d'escalade, etc.
- Nous recommandons à la Ville de mettre en place un système d'analyse des journaux et d'alertes lui permettant d'être mise au courant en temps réel s'il y a des tentatives d'accès ou des incidents de sécurité.
- Nous recommandons à la Ville d'élaborer un plan de relève TI qui va comprendre la liste des actifs critiques, leur temps d'interruption maximum (RTO) et la perte maximale de données (RPO), les principaux acteurs, les étapes de relève, etc.

  La définition des indicateurs RTO et RPO devra résulter d'une analyse d'impacts sur les affaires réalisée de connivence avec les autres services de la Ville.

3.3.4. Gestion des fournisseurs

La Ville collabore avec des fournisseurs qui peuvent héberger des RP, et ce, collectés au bénéfice de la Ville. Dans le cas de Sport-Plus, il s'agit d'une application hébergée et gérée par le fournisseur, et donc, des RP de citoyens (p. ex. : nom, prénom, date de naissance, courriel, adresse, code postal, téléphone, sexe, langue, numéro de carte d'assurance maladie, NAS, etc.) peuvent se retrouver chez celui-ci.

Considérant que des RP collectés pour la Ville sont hébergés chez des fournisseurs, il est important pour la Ville de mettre en place un processus formel de gestion des fournisseurs afin de s'assurer que les fournisseurs avec qui la Ville collabore répondent aux standards établis en matière de sécurité et de protection des RP. De plus, la Ville doit mettre en place des mesures de surveillance afin d'évaluer la conformité de ces fournisseurs aux standards établis. Nous avons noté que la Ville n'a pas mis en place un processus formel de gestion des fournisseurs permettant de s'assurer que les bonnes pratiques de sécurité sont prises en compte dans les contrats. En ce qui concerne le fournisseur de l'application Sport-Plus, il est à noter que le contrat avec celui-ci stipule qu'il s'engage à assurer la confidentialité des RP qu'il héberge.

Aussi, la Ville ne procède pas à une évaluation périodique de ses fournisseurs afin d'identifier les fournisseurs les plus à risque selon les RP hébergés et afin d'évaluer la sécurité par l'entremise d'un questionnaire ou l'obtention d'une attestation externe démontrant leur conformité à un cadre de référence reconnu.

Recommandations

- Nous recommandons à la Ville de mettre en place un processus formel de gestion des fournisseurs critiques afin de définir le processus lors de la sélection d'un nouveau fournisseur et d'évaluer périodiquement la performance et la conformité de celui-ci aux standards de sécurité établis et attendus. L'évaluation périodique doit être effectuée en fonction du risque associé au fournisseur afin de s'assurer qu'il respecte les clauses contractuelles et les standards établis en matière de sécurité et de protection des RP.
- Nous recommandons à la Ville d'intégrer des clauses au contrat de service auprès des nouveaux fournisseurs critiques relativement aux attentes en matière de sécurité et de protection des RP ainsi qu'aux divulgations nécessaires en cas de bris de confidentialité. Voici une liste non exhaustive de clauses à considérer :
    - Accès aux RP restreint au personnel autorisé du fournisseur;
    - Confidentialité des RP hébergés;
    - Sous-traitants du fournisseur (si applicable) devant se conformer aux mêmes standards de sécurité que le fournisseur selon le contrat;
    - Durée de conservation des RP et méthodes de destruction;
    - Etc.

4. Conclusion

La Ville possède plusieurs RP, autant sur ses employés que ses citoyens. La Ville doit donc s'assurer de mettre en place un environnement de contrôle adéquat permettant de maintenir la confidentialité des RP et de protéger ceux-ci.

En conclusion, bien que la Ville ait mis en place plusieurs mesures visant la protection des RP, celles-ci pourraient, à notre avis, faire l'objet d'améliorations et d'une optimisation des ressources de la Ville.

Gouvernance

Critère – La Ville dispose de politiques définissant les exigences quant à la gestion des RP, et ce, pour l'ensemble des services de la Ville.

Nous pouvons conclure que la Ville dispose de politiques définissant les exigences quant à la gestion des RP. En effet, la Ville a élaboré une politique de confidentialité, sa *Politique-cadre sur la gouvernance des renseignements personnels,* ainsi que certaines politiques/directives définissant certaines exigences en matière de sécurité TI et de gestion des RP. Cependant, la Ville devra bonifier ses politiques en matière de sécurité de l'information et devra élaborer une politique de confidentialité et de gestion des témoins (*cookies*).

De plus, la Ville a adopté la mise en place d'un comité sur l'accès à l'information et la protection des renseignements personnels et nommé un responsable de l'accès et de la protection des renseignements personnels, également responsable de l'accès aux documents, et ce, comme exigé par la loi 25. Les règles de fonctionnement du comité seront cependant à établir.

Critère – La Ville maintient un inventaire des RP, permettant à celle-ci d'avoir un portrait global des renseignements à protéger.

Nous pouvons conclure que bien que la Ville ait mis en place un inventaire des actifs informationnels, celui-ci ne détaille pas l'inventaire des systèmes ni les informations sur les RP qu'ils contiennent. De plus, les documents papiers conservés et les RP qu'ils contiennent ne sont pas inventoriés.

Finalement, aucun mécanisme n'est en place permettant de répondre à une demande d'un citoyen ou d'un employé en ce qui concerne les renseignements personnels collectés, traités et conservés, incluant les fins pour lesquelles les données sont conservées, et ce, dans les délais prescrits.

Critère – Les employés de la Ville sont sensibilisés quant aux enjeux et risques liés à la gestion des RP afin que ceux-ci respectent les politiques ou mesures visant la sécurité de ces renseignements.

Nous pouvons conclure que la Ville a mis en place un programme de sensibilisation auprès des employés permettant de mener des campagnes de sensibilisation, des campagnes de simulations d'hameçonnage ainsi que de produire des bulletins d'information. Cependant, il n'y a pas eu de campagnes de sensibilisation formelles ou de formations sur la sécurité de l'information et des RP auprès de l'ensemble des employés de la Ville.

Conservation et destruction des RP

Les RP sont conservés selon un calendrier préétabli et lorsque ceux-ci ne sont plus requis, ils sont détruits de manière à ce qu'ils ne puissent plus être reconstitués.

Nous pouvons conclure que la Ville a établi un plan de classification qui contient le recueil des délais de conservation des données, dont les RP. Une durée de vie est attribuée selon la nature du document afin de déterminer les documents (supports papier ou électronique) à archiver, à conserver ou à détruire.

De plus, concernant la destruction des archives et des données électroniques, celles-ci sont détruites de manière à ce qu'elles ne puissent plus être reconstituées.

Mesures de protection

Critère – Les accès sont accordés de manière à ce que les accès aux RP soient limités aux personnes autorisées uniquement, par leurs rôles et responsabilités. De plus, les paramètres de sécurité sont assez robustes pour prévenir des accès non autorisés aux RP.

Nous pouvons conclure que bien que certains mécanismes soient en place afin d'assurer que les accès soient accordés aux personnes autorisées uniquement, certains paramètres de sécurité permettent de prévenir des accès non autorisés aux RP. Ces mécanismes pourraient être améliorés :

- Formaliser le processus d'octroi d'accès et de modification des accès pour les applications et les serveurs de fichiers, incluant l'autorisation du propriétaire de l'application avant d'octroyer un accès, et ce, pour l'ensemble des applications;
- Restreindre au service des TI la capacité de gérer les accès aux applications;
- Mise en place d'un processus formel afin d'aviser le service des TI et les responsables applicatifs lors du départ d'un employé, et ce, pour assurer le retrait des accès en temps opportun;
- Éviter ou minimiser l'utilisation de comptes génériques ou, pour les situations où ces comptes sont requis, contrôler l'utilisation de ceux-ci, et ce, afin d'assurer l'imputabilité des actions commises;
- Gérer les droits d'accès par groupe au lieu de droits à la pièce afin de faciliter la gestion et la révision des accès;
- Mise en place d'un processus formel de révision périodique des accès, incluant une revue complète des utilisateurs et de leurs rôles pour s'assurer de la juste séparation des tâches et que l'accès aux RP, autant en lecture qu'en écriture, est restreint au personnel approprié;
- Établir une politique de mots de passe alignée aux bonnes pratiques en matière d'authentification.

Critère – La Ville a mis en place des mesures de surveillance afin de prévenir et de détecter des attaques ou des vulnérabilités potentielles. De plus, la Ville procède à des tests d'intrusion qui permettent de mesurer les vulnérabilités des systèmes contenant des RP face aux cyberattaques.

Nous pouvons conclure que les mesures de surveillance en place sont suffisantes afin de prévenir et de détecter des attaques ou des vulnérabilités potentielles. Cependant, la Ville devrait procéder à des tests d'intrusion qui permettent de mesurer les vulnérabilités des systèmes contenant des RP face aux cyberattaques, et ce, périodiquement.

Critère – La Ville a mis en place un processus de gestion des incidents lui permettant de réagir en temps opportun en cas d'incident majeur visant des RP afin de minimiser les impacts réels d'un tel incident et de prendre les mesures nécessaires afin de résoudre celui-ci.

Nous pouvons conclure que la Ville n'a pas mis en place de processus formel décrivant le cadre pour la détection et les niveaux d'escalade en cas d'incident de sécurité et de bris de RP. De plus, les incidents ou problèmes ne sont pas formellement journalisés dans un système de billetterie, ce qui permettrait d'avoir une vue globale des incidents et d'identifier les tendances ou les incidents récurrents.

Critère – Les RP transmis, gérés ou hébergés par de tierces parties (fournisseurs) sont protégés afin de préserver la confidentialité de ceux-ci.

Nous pouvons conclure qu'en ce qui concerne la gestion des fournisseurs, ceux-ci pouvant héberger des RP collectés au bénéfice de la Ville, aucun processus formel n'est en place pour la gestion de ceux-ci afin de définir le processus lors de la sélection d'un nouveau fournisseur et d'évaluer périodiquement la performance et la conformité de celui-ci aux standards de sécurité établis et attendus. De plus, il n'y a pas systématiquement de clauses au contrat de service auprès de ces fournisseurs en ce qui concerne les attentes en matière de sécurité et de protection des RP, ainsi qu'aux divulgations nécessaires en cas de violation de confidentialité.

5. Objectif et critères d'audit

5.1. OBJECTIF

S'assurer que les renseignements personnels détenus par la Ville faisaient l'objet d'une protection adéquate afin de mitiger les risques de bris de confidentialité, de vol ou d'accès non autorisés aux RP.

5.2. CRITÈRES D'AUDIT

- Gouvernance :
  - La Ville dispose de politiques définissant les exigences quant à la gestion des RP, et ce, pour l'ensemble des services de la Ville;
  - La Ville maintient un inventaire des RP, permettant à celle-ci d'avoir un portrait global des renseignements à protéger;
  - Les employés de la Ville sont sensibilisés quant aux enjeux et risques liés à la gestion des RP afin que ceux-ci respectent les politiques ou mesures visant la sécurité de ces renseignements;
- Conservation et destruction des RP :
  - Les RP sont conservés selon un calendrier préétabli et lorsque ceux-ci ne sont plus requis, ils sont détruits de manière à ce qu'ils ne puissent plus être reconstitués;
- Mesures de protection à l'égard des RP :
  - Les accès sont accordés de manière à ce que les accès aux RP soient limités aux personnes autorisées uniquement, de par leurs rôles et responsabilités. De plus, les paramètres de sécurité sont assez robustes pour prévenir des accès non autorisés aux RP;
  - La Ville a mis en place des mesures de surveillance afin de prévenir et de détecter des attaques ou des vulnérabilités potentielles. De plus, la Ville procède à des tests d'intrusion qui permettent de mesurer les vulnérabilités des systèmes contenant des RP face aux cyberattaques;
  - La Ville a mis en place un processus de gestion des incidents lui permettant de réagir en temps opportun en cas d'incident majeur visant des RP afin de minimiser les impacts réels d'un tel incident et de prendre les mesures nécessaires afin de résoudre celui-ci;
  - Les RP transmis, gérés ou hébergés par de tierces parties (fournisseurs) sont protégés afin de préserver la confidentialité de ceux-ci.

rcgt.com

Raymond Chabot Grant Thornton

Certification | Fiscalité | Conseil