Rapport annuel 2024

Vérificatrice générale de la Ville de Lévis

Lévis | VÉRIFICATEUR GÉNÉRAL

ville.levis.qc.ca

Lévis | VÉRIFICATEUR GÉNÉRAL

Lévis, le 14 juillet 2025

Monsieur Gilles Lehouillier
Maire de la Ville de Lévis
2175 Chemin du Fleuve
Lévis (Québec) G6W 7W9

Objet : Dépôt du rapport annuel de la vérificatrice générale de la Ville de Lévis pour l'exercice terminé le 31 décembre 2024

Monsieur le Maire,

Conformément à l'article 107.13 de la *Loi sur les cités et villes* (RLRQ, chapitre C-19), je vous transmets mon rapport annuel, pour l'exercice terminé le 31 décembre 2024, et ce, pour dépôt à la prochaine séance ordinaire du conseil municipal, soit celle du 14 juillet 2025.

Ce rapport inclut le rapport de l'auditeur indépendant sur le relevé des dépenses d'opérations du Bureau du vérificateur général de Lévis.

Je vous prie d'agréer, Monsieur le Maire, l'expression de mes sentiments distingués.

La vérificatrice générale de la Ville de Lévis,

(Original signé par la vérificatrice générale)

Francine Tessier, CPA Auditrice,
Permis de comptabilité publique no A107892
Lévis (Québec), Canada

Table des matières

Message de la vérificatrice générale

CHAPITRE 1

Lévis | VÉRIFICATEUR GÉNÉRAL

Message de la vérificatrice générale

En janvier 2024, j'ai entrepris mon mandat de sept ans à titre de vérificatrice générale de la Ville de Lévis, animée par le désir de soutenir l'administration municipale dans l'exercice d'une gestion rigoureuse et transparente, au bénéfice des citoyennes et citoyens. Je tiens à exprimer ma sincère reconnaissance aux membres du conseil municipal pour la confiance qu'ils m'ont témoignée lors de ma nomination.

Ce rapport public, le premier que je présente dans le cadre de mes fonctions, reflète l'engagement du Bureau de la vérificatrice générale à exercer sa mission avec objectivité, indépendance et rigueur.

Mandat de la vérificatrice générale

La vérificatrice générale a la responsabilité d'effectuer, dans la mesure qu'elle juge appropriée, la vérification des comptes et affaires de la Municipalité et des organismes visés par la *Loi sur les cités et villes* (LCV). Cette vérification peut prendre la forme d'un audit financier, d'un audit d'optimisation des ressources ou d'un audit de conformité aux lois, règlements et politiques.

Par ses travaux et ses rapports accessibles au public, la vérificatrice générale porte un regard objectif et indépendant sur la qualité de la gestion de la Ville, de ses fonds publics et de sa prestation de services aux citoyens et citoyennes. Elle contribue à accroître le degré d'imputabilité du pouvoir exécutif de la Municipalité ainsi que sa transparence en matière fiscale et comptable. Les audits ne sont pas effectués dans l'objectif de mettre en cause le bien-fondé des politiques et objectifs de la Municipalité ou des organismes.

Rapport 2024

Le rapport annuel 2024 rend compte des travaux suivants :

- **Chapitre 2** Gestion des risques liés à la protection des renseignements personnels
- **Chapitre 3** Contrôles généraux informatiques
- **Chapitre 4** Organismes ayant bénéficié d'une subvention d'au moins 100 000 $
- **Chapitre 5** Suivi de l'implantation des recommandations formulées lors d'audits antérieurs
- **Annexe** Relevé des dépenses d'opération du Bureau de la vérificatrice générale

Ce rapport vise à offrir une vue d'ensemble transparente des interventions réalisées pour l'année 2024, au bénéfice des instances municipales et, surtout, de la population lévisienne.

Membre de l’Ordre des comptables professionnels agréés du Québec

La vérificatrice générale, en tant que CPA Auditrice membre de l’Ordre des comptables professionnels agréés du Québec (OCPAQ), se conforme aux règles et au code de déontologie applicables à l’exercice de ses fonctions, lesquels reposent sur les principes fondamentaux d’intégrité, d’objectivité, de compétence professionnelle et de diligence, de confidentialité et de conduite professionnelle. La vérificatrice générale applique les Normes canadiennes de gestion de la qualité.

L’OCPAQ veille à ce que ses membres respectent les normes élevées de compétence et d’éthique, grâce à des formations continues et à des processus rigoureux d’admission et de surveillance. La vérificatrice générale rend des comptes à l’OCPAQ conformément aux exigences de ces processus.

Remerciement

Je remercie le personnel de la Ville qui a collaboré aux travaux d’audit en fournissant des réponses complètes et des suggestions constructives.

Je tiens à souligner l’engagement des personnes au sein de l’équipe du Bureau de la vérificatrice générale ainsi que tous les professionnels externes qui ont travaillé à la réalisation des différentes missions d’audit.

Je remercie les vérificatrices et vérificateurs généraux des grandes villes du Québec pour l’information et les conseils, particulièrement pour la mise en place du Bureau de la vérificatrice générale.

Je remercie sincèrement les citoyens qui ont transmis de l’information pour contribuer aux travaux d’audit. Notez que les informations recueillies au cours de l’audit, incluant l’identité des personnes y ayant contribué en fournissant de l’information, demeurent confidentielles.


Lévis
VÉRIFICATEUR
GÉNÉRAL

Gestion des risques liés à la protection des renseignements personnels

Audit de performance

CHAPITRE 2

Lévis | VÉRIFICATEUR GÉNÉRAL

2

Gestion des risques liés à la protection des renseignements personnels

Audit de performance

Table des matières

Liste des acronymes

CAI	Commission d'accès à l'information du Québec
CAIPRP	Comité sur l'accès à l'information et la protection des renseignements personnels
DG	Direction générale
DIC	Disponibilité, intégralité, confidentialité
DTITN	Direction des technologies de l'information et de la transformation numérique
ÉFVP	Évaluation des facteurs relatifs à la vie privée
PQI	Programme quinquennal des immobilisations
PRP	Protection des renseignements personnels
RLRQ	Recueil des lois et des règlements du Québec
RP	Renseignement personnel
RAPRP	Responsable de l'accès aux documents et de la protection des renseignements personnels
VG	Vérificatrice générale

Synthèse des travaux d'audit

Contexte :

Pour accomplir sa mission, la Ville de Lévis (ou « la Ville ») recueille des renseignements personnels (RP), dont certains sont sensibles. La conformité à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ci-après « la Loi sur l'accès ») fait partie des obligations que la Direction générale (DG) doit considérer dans l'allocation des ressources pour atteindre ses objectifs.

La DG a choisi d'appliquer les principes de gestion des risques pour prendre des décisions éclairées et prioriser les travaux à effectuer au regard des exigences de la Loi sur l'accès. La DG a confié le mandat de la gestion des risques corporatifs à la Direction de la planification stratégique et de l'amélioration continue. Une approche structurée de gestion des risques, inspirée des principes de la norme internationale ISO 31000, permet d'accroître la probabilité d'atteindre les objectifs stratégiques, d'améliorer la gouvernance et de renforcer l'efficacité opérationnelle. Elle favorise une culture où le risque devient un levier de planification et d'innovation.

Objectifs :

Cet audit visait à assurer que la méthodologie de gestion des risques liés aux RP permet de bien identifier, évaluer et mitiger les risques de non-conformité aux exigences légales et règlementaires, en fonction de la criticité, ainsi que d'affecter les ressources nécessaires pour effectuer les travaux selon les priorités établies.

Résultats :

La Ville a amorcé une démarche concrète pour rehausser sa conformité aux exigences de la Loi sur l'accès. Plusieurs actions structurantes ont été réalisées, et un budget de 2 075 000 $ a été inscrit au Programme quinquennal des immobilisations (PQI) pour des initiatives en lien avec la protection des RP (PRP). La DG a également pris position pour prioriser les travaux de gestion des risques liés aux RP des citoyens et citoyennes.

Le développement du cadre organisationnel et de la méthodologie de gestion des risques liés aux RP est en phase de conception. En conséquence, le modèle de gestion des risques, la structure de gouvernance, les plans d'action et les ressources nécessaires n'ont pas encore été définis. Notons que la méthodologie d'évaluation des facteurs relatifs à la vie privée (ÉFVP) proposée par la Commission d'accès à l'information du Québec (CAI) a été adoptée par la DG et appliquée une première fois au printemps 2025, avec succès. Cette ÉFVP est effectuée notamment dans le contexte spécifique d'un projet d'acquisition, de développement et de refonte d'un système d'information ou de la prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de RP.

L'analyse des besoins de formation en gestion des risques, outre la formation applicable dans le contexte de l'ÉFVP, n'a pas été effectuée, et aucune formation n'a été offerte à cet égard. Les employés et employées qui devront contribuer à l'analyse des risques des RP de la population ont besoin de recevoir une telle formation.

Les responsabilités du CAIPRP sont en train d'être redéfinies à la suite de la nouvelle mission attribuée à la Direction des technologies de l'information, devenue Direction des technologies de l'information et de la transformation numérique (DTITN). La réévaluation des responsabilités de cette direction quant à la prise en charge des incidents informatiques impliquant des RP génère de l'ambiguïté sur les responsabilités des intervenants et intervenantes.

Contexte

Les municipalités jouent un rôle essentiel dans la qualité de vie des Québécoises et des Québécois. Elles assurent une multitude de services essentiels – de l'eau potable à la voirie, en passant par les loisirs, la sécurité (publique, civile et incendie) et l'aménagement du territoire. Elles interviennent dans des domaines aussi variés que la lutte aux changements climatiques, le logement, la mobilité durable, l'inclusion sociale et la vitalité économique régionale. Elles sont des actrices de premier plan dans la mise en œuvre de réponses concrètes aux grands enjeux contemporains.

Pour accomplir sa mission, la Ville de Lévis recueille des renseignements personnels (RP), dont certains sont sensibles, qu'elle utilise comme source d'information pour identifier une personne et connaitre ses besoins et ses préférences en vue de mieux la servir. Les principales personnes concernées par ces renseignements sont les citoyens et citoyennes, les membres du personnel et du conseil municipal et le personnel des partenaires (organismes liés, fournisseurs et autres partenaires).

Les RP sont les renseignements qui permettent d'identifier, directement ou indirectement, une personne physique. Un renseignement qui ne permet pas d'identifier un individu peut constituer un RP si, jumelé à d'autres renseignements, il permet de l'identifier. Il est qualifié de sensible lorsque sa nature ou le contexte de son utilisation ou de sa communication suscite un haut degré d'attente raisonnable en matière de vie privée. S'ils sont de nature médicale, biométrie ou autrement intimes, les RP sont généralement considérés comme sensibles.

La conformité aux exigences de la Loi sur l'accès fait partie des obligations que la DG doit considérer lorsqu'elle alloue les ressources pour accomplir sa mission, en assurant une saine administration des deniers publics.

La conformité aux exigences de la Loi sur l'accès fait partie des obligations que la direction générale doit considérer lorsqu'elle alloue les ressources pour accomplir sa mission, en assurant une saine administration des deniers publics.

La Loi sur l'accès encadre la gestion des RP tout en visant à créer un équilibre entre deux principes fondamentaux : l'accès à l'information pour favoriser la transparence, et la protection de la vie privée des individus en ce qui concerne l'utilisation de leurs RP. La Loi sur l'accès s'applique aux informations détenues par la Ville dans l'exercice de ses fonctions, même lorsque leur conservation est assurée par un tiers.

Principaux changements législatifs en matière de PRP

Le gouvernement du Québec a sanctionné, en septembre 2021, la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (communément désignée la « Loi 25 »). Depuis, les amendements ont été directement intégrés dans le texte de la Loi sur l'accès, en vigueur depuis 1982. Voici les principaux changements apportés à la Loi sur l'accès, promulguée en 2021 :

Nomination obligatoire d'un responsable PRP

L'organisme doit aviser la CAI par écrit du titre, des coordonnées et de la date d'entrée en fonction de la personne qui exerce la fonction de responsable de la PRP.

Évaluation des facteurs relatifs à la vie privée (ÉFVP)

La Loi sur l'accès prévoit les circonstances dans lesquelles une ÉFVP doit être effectuée pour évaluer les risques du point de vue des individus et sélectionner des mesures pour que ces risques soient à un niveau acceptable pour ces individus. L'ÉFVP doit être proportionnée à la sensibilité des renseignements concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support, et être effectuée en concertation avec le ou la responsable de la PRP.

Création d'un comité sur l'accès à l'information et la protection des renseignements personnels (CAIPRP)

Le CAIPRP soutient le ou la responsable de la PRP, approuve les règles de gouvernance et donne son avis sur les projets ayant un impact sur la vie privée, incluant les ÉFVP.

Déclaration obligatoire des incidents de confidentialité

Un registre des incidents doit être maintenu, et la Ville doit aviser sans délai la CAI et les personnes concernées si l'incident présente un risque de préjudice sérieux.

Des mesures raisonnables doivent être prises pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature se reproduisent.

Information sur les décisions fondées exclusivement sur un traitement automatisé de renseignements personnels

Un organisme public qui utilise des RP afin que soit rendue une décision fondée exclusivement sur un traitement automatisé de ceux-ci doit en informer la personne concernée au plus tard au moment où il l'informe de cette décision et fournir les autres informations exigées par la Loi sur l'accès.

Rehaussement des exigences de transparence

Un organisme public doit publier sur son site Internet :

- les règles encadrant sa gouvernance à l'égard des RP. Ces règles doivent être approuvées par son CAIPRP;
- une politique de confidentialité rédigée en termes simples et clairs.

Information concernant les produits ou services technologiques disposant de paramètres de confidentialité

Les produits ou services technologiques offerts aux citoyens et citoyennes et qui permettent à la Ville de recueillir des RP doivent, par défaut, offrir le plus haut niveau de confidentialité, sans aucune intervention des personnes concernées.

Renforcement des règles entourant le consentement

Le consentement doit être manifeste, libre, éclairé, donné à des fins précises, et demandé en termes simples et clairs. Il ne vaut que pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé. Sauf exceptions, la Ville ne peut communiquer un RP sans le consentement de la personne concernée. Si elle recueille des RP en ayant recours à une technologie comprenant des fonctions permettant d'identifier, de localiser ou d'effectuer un profilage, elle doit informer les personnes de l'utilisation d'une telle technologie et des moyens offerts pour activer ces fonctions.

Le consentement d'une personne de moins de 14 ans est donné par le ou la titulaire de l'autorité parentale ou par le tuteur ou la tutrice.

Un consentement qui n'est pas donné conformément à la Loi sur l'accès est sans effet.

Droit à la portabilité

Sur demande de la personne concernée, la Ville doit pouvoir lui communiquer les RP recueillis auprès d'elle dans un format technologique structuré et couramment utilisé, sauf si cela soulève des difficultés pratiques sérieuses. Ces RP peuvent être communiqués à toute personne ou tout organisme désigné par la personne concernée.

Transformation numérique à la Ville de Lévis

La majorité des RP sont aujourd'hui conservés en format numérique. Il est donc raisonnable de penser que la DTITN aura un rôle important à jouer dans les changements à apporter pour assurer la conformité règlementaire.

La DG vient de commencer, avec l'arrivée en poste du directeur de la DTITN, ses réflexions vers une transformation numérique pour faire des TI un levier de performance, d'innovation et de résilience. Les changements dans les processus d'affaires requis pour renforcer la conformité à la Loi sur l'accès doivent être coordonnés avec la transformation numérique pour que ces changements répondent aux besoins à long terme. Cela n'empêche pas la Ville de réaliser des actions dès maintenant, dans une démarche cohérente vers la conformité à la Loi sur l'accès dans un horizon de temps raisonnable.

La transformation numérique et les investissements technologiques qui l'accompagnent en infrastructures TI, en solutions infonuagiques, en logiciels métiers et en technologies avancées (IA, automatisation robotisée, Internet des objets, etc.) sont une opportunité pour minimiser les contraintes opérationnelles dans la démarche de conformité à la Loi sur l'accès.

La gestion des risques pour prendre les décisions

Le Secrétariat du Conseil du trésor a publié, en mars 2022, les *Orientations en matière de gestion intégrée des risques dans l'administration gouvernementale*, précisant que cette approche « permet notamment d'accroître la probabilité pour une organisation d'atteindre ses objectifs stratégiques, de parfaire sa gouvernance et d'améliorer son efficacité et son efficience opérationnelle ». Ces orientations ne s'appliquent pas directement aux municipalités, mais elles peuvent certainement les inspirer.

Lorsque la *Loi sur les contrats des organismes publics* (LCOP) a été promulguée, le gouvernement du Québec a recommandé aux organisations assujetties d'appliquer les principes de gestion des risques afin d'établir leurs plans d'action.

Le texte de la Loi sur l'accès décrit clairement les cibles à atteindre, mais la feuille de route optimale pour y parvenir doit être établie par le ou la responsable de la PRP de chaque organisation. Le gouvernement du Québec propose une feuille de route, mais précise qu' « [é]tant donné le contexte particulier de chaque organisme public, les éléments à réaliser sont présentés à haut niveau, par défaut. Un organisme public peut les adapter en fonction de sa propre réalité.[1] »

Adopter une approche structurée de gestion des risques, inspiré des principes de la norme ISO 31000, implique de favoriser une culture organisationnelle où le risque n'est plus perçu comme un frein, mais plutôt comme un levier de planification et d'innovation.

La DG de la Ville de Lévis a décidé d'appliquer les principes de gestion des risques pour prendre des décisions éclairées et prioriser les travaux à effectuer au regard des exigences de la Loi sur l'accès.

La DG de la Ville a décidé d'appliquer les principes de gestion des risques pour prendre des décisions éclairées et prioriser les travaux à effectuer au regard des exigences de la Loi sur l'accès.

[1] Ministère du Conseil exécutif, *Éléments qu'un organisme public doit réaliser pour se conformer aux modifications prévues par la loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, p. 1.

Principales composantes de la gestion des risques

En matière de gestion des risques, plusieurs référentiels sont largement reconnus et utilisés à travers le monde, offrant des cadres et des bonnes pratiques pour aider les organisations à identifier, évaluer et traiter les risques. La gestion des risques améliore la performance, favorise l'innovation et contribue à l'atteinte des objectifs. Les lignes directrices ISO 31000:2018, référentiel le plus couramment utilisé, reposent sur les trois composantes suivantes :

- les 8 principes de gestion des risques;
- le cadre organisationnel;
- le processus de gestion des risques (méthodologie structurée).

I. Principes essentiels de gestion des risques

Voici les principes essentiels pour une gestion des risques efficace en PRP :

- Elle doit suivre une approche méthodique, complète et cohérente dans toute l'organisation.
- La participation des parties prenantes est essentielle à une gestion des risques efficace et réaliste.
- Les besoins, la taille, la structure et les enjeux de l'organisation doivent être pris en compte.

II. Cadre organisationnel

L'objectif du cadre organisationnel de la gestion des risques est d'aider la Ville à intégrer le risque dans ses activités et ses fonctions importantes. L'efficacité de la gestion des risques va dépendre de son intégration dans la gouvernance de la Ville, y compris lors de la prise de décision. Voici les principaux éléments du cadre organisationnel de gestion des risques :

1. Les dirigeants doivent montrer l'exemple, fournir des ressources et présenter un alignement stratégique.
2. La gestion des risques doit s'insérer dans tous les processus décisionnels.
3. Il faut comprendre le contexte et définir les rôles.
4. Le cadre doit être déployé opérationnellement.
5. La performance, les résultats et le niveau de maturité doivent être mesurés.
6. Il faut procéder à des ajustements en réponse aux évaluations, aux incidents ou aux changements.

III. Processus de gestion des risques (méthodologie)

Voici les principales étapes du processus pour assurer une gestion rigoureuse et structurée des risques :

1. Établir le contexte interne (structure, culture, objectifs) et externe (environnement, lois, parties prenantes).
2. Identifier les risques.
3. Analyser les risques sur les plans de la probabilité, des impacts, des causes et des interdépendances.
4. Évaluer les risques selon des critères approuvés par la DG.
5. Choisir le traitement des risques : éliminer, réduire, transférer, accepter ou éviter.
6. Effectuer une veille en continu pour détecter l'évolution des circonstances.
7. Communiquer avec toutes les parties concernées et les consulter en maintenant un dialogue constant avec elles.

Principaux risques et enjeux

Principaux risques

Incident de confidentialité causant un préjudice sérieux

Risque que les RP des citoyens et citoyennes ou du personnel soient divulgués (à la suite d'une cyberattaque, d'un vol ou d'une erreur internes, etc.) et que ceci entraine un préjudice sérieux aux personnes concernées.

Mauvaises utilisations des RP

Risque d'utilisation des RP sans consentement et transparence adéquate, d'abus de pouvoir ou de surveillance excessive. Par exemple, l'usage de la vidéosurveillance doit demeurer proportionnel au risque et être justifié pour répondre à un réel besoin.

Non-respect des engagements budgétaires et opérationnels

Risque qu'un incident de confidentialité nécessite un investissement budgétaire important pour gérer la crise qui en résulte et pour maintenir les services à la population.

Risque que les sommes engagées pour mitiger les risques liés aux RP ne soient pas investies de façon optimale pour réduire ces risques d'une façon pérenne.

Réputation

Risque de perte de confiance des citoyens à la suite d'un préjudice lors de la collecte, du vol ou de l'utilisation de RP ou de l'incapacité de prouver l'identité de la personne responsable du préjudice. Les citoyens et citoyennes pourraient alors être réticents à fournir les RP demandés en vue d'obtenir les services dont ils et elles ont besoin.

Principaux enjeux

Limitations technologiques

La majorité des RP sont conservés en format numérique, et leur gestion est tributaire, au moins en partie, des limitations technologiques des systèmes d'information telles que les fonctionnalités pour gérer les droits d'accès et l'interconnexion de ces systèmes.

Dépendance des fournisseurs

Lorsque des fournisseurs gèrent des outils ou des applications utilisés par la Ville pour héberger les RP, ils doivent fournir l'information nécessaire pour analyser les risques.

Résistance au changement

Plusieurs exigences de la Loi sur l'accès, dont l'intégration des mesures de sécurité dès la conception d'un projet, impliquent des changements dans les façons de faire qui nécessiteront l'appui ferme de la DG pour que les parties prenantes dépassent leurs réticences naturelles.

Contraintes opérationnelles et stratégiques

Pour se conformer à la Loi sur l'accès, la Ville doit arrimer les changements requis aux processus d'affaires et aux systèmes informatiques avec les changements aux processus par ailleurs nécessaires à la mise en œuvre des projets déjà planifiés dans les orientations stratégiques. Cet enjeu est accentué par l'important chantier de transformation numérique en cours à la Ville.

Apprentissage en gestion des risques

La Ville de Lévis a peu d'expérience en gestion des risques, telle que définie dans les lignes directrices ISO 31000, et sera donc en apprentissage pour concevoir son cadre organisationnel, sa méthodologie et ses outils de travail de gestion des risques en PRP.

Apprentissage en intelligence artificielle

La Ville de Lévis est en apprentissage à cet égard et doit relever de nombreux défis, notamment ceux de maintenir la qualité des RP et de choisir les données d'entrainement pour que leur utilisation soit éthique, que les décisions garantissent l'équité et la non-discrimination, etc.

Capacité organisationnelle

La Ville doit allouer la capacité organisationnelle pour maintenir les services aux citoyens et citoyennes, poursuivre les initiatives prévues au PQI et rehausser le niveau de PRP tout en respectant ses contraintes budgétaires. Les processus n'étant pas documentés, plusieurs consultations sont requises avec les directions concernées pour qu'elles fournissent de l'information en vue d'une compréhension suffisante.

Information à la population

La population de la Ville de Lévis se caractérise par sa diversité culturelle, générationnelle et sociale. Cette diversité pose des défis de communication lorsqu'il s'agit de transmettre une information simple et claire, d'obtenir un consentement manifeste, libre et éclairé, et d'assurer que les citoyens et citoyennes comprennent bien les implications de leur acceptation ou de leur refus.

Résultat de l'audit

La DG de la Ville de Lévis a pris des mesures concrètes afin de rehausser sa conformité aux obligations découlant de la Loi sur l'accès. La démarche, bien enclenchée, est toujours en phase de consolidation. Voici les principales actions effectuées :

Des mesures concrètes ont été prises afin de rehausser la conformité aux obligations découlant de la Loi sur l'accès. La démarche, bien enclenchée, est toujours en phase de consolidation.

- Création, en avril 2022, du CAIPRP, dont les membres se sont réunis régulièrement sous la présidence du directeur général;
- Approbation, par la DG et le conseil municipal, de la plupart des pièces de gouvernance requise par la Loi sur l'accès. La politique de sécurité de l'information et la directive sur les sondages sont en voie d'être finalisées;
- Sensibilisation sur la PRP et la sécurité informatique auprès de tout le nouveau personnel qui possède une adresse courriel de la Ville;
- Formation pour rehausser les connaissances sur la PRP des gestionnaires et des membres du personnel appelés à jouer un rôle clé; à la suite des formations en PRP et en sécurité de l'information, ils et elles ont les connaissances nécessaires pour contribuer à l'analyse des risques dans leur service;
- Formation de 43 membres du personnel sur les outils et techniques nécessaires pour préparer une ÉVFP;
- Réalisation d'une ÉVFP détaillée sur la vidéosurveillance, dans le complet respect des règles de l'art;
- Décision de la DG de prioriser les travaux de gestion des risques avec les RP des citoyens et citoyennes;
- Budget de 2 075 000 $ inscrit au PQI.

Ces efforts traduisent la volonté claire de la Ville de maitriser les risques associés aux RP collectés auprès des citoyens et citoyennes, sur tout le cycle de vie.

Conclusion générale

La Ville étant encore au début de sa montée en maturité, nous concluons que la méthodologie de gestion des risques liés aux RP ne permet pas encore de bien identifier, évaluer et mitiger les risques de non-conformité aux exigences légales et règlementaires, en fonction de la criticité, ni d'affecter les ressources nécessaires pour effectuer les travaux selon les priorités établies

Notons que la méthodologie d'ÉFVP proposée par CAI adoptée par la DG a été appliquée une première fois au printemps 2025, avec succès. Cette ÉFVP est effectuée notamment dans le contexte d'un projet d'acquisition, de développement et de refonte d'un système d'information ou de la prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de RP.

Opportunités d'amélioration et recommandations

La section qui suit détaille les principales opportunités d'amélioration et les recommandations pour chacun des critères d'audit.

Critère 1 : La gestion des risques liés aux RP est effectuée selon une approche systématique et structurée

Opportunités d'amélioration

La démarche de gestion des risques liés aux RP n'est pas définie; le développement du cadre organisationnel et de la méthodologie de gestion des risques liés aux RP est en phase de conception.

RECOMMANDATIONS

1. Établir le modèle de gestion des risques liés aux RP, concevoir les outils adaptés aux risques liés à la PRP (disponibilité, intégralité, confidentialité, ou « DIC ») et à l'ensemble du cycle de vie (collecte, utilisation, communication, disposition) en y intégrant les exigences des directives sur la gestion des incidents de confidentialité des RP et sur la gestion des ÉFVP.
2. Effectuer l'analyse des risques liés aux RP. Dresser le plan d'action et le calendrier de réalisation pour prioriser les interventions. Obtenir l'approbation de la DG, du ou de la RPRP et du CAIPRP sur le plan d'action et le risque résiduel avant de commencer la revue des processus.
3. Formaliser la reddition de comptes de la gestion des risques liés aux RP : définir le format, les destinataires et la fréquence de cette reddition. Identifier les personnes ayant la responsabilité de la produire.

Critère 2 : La structure de gouvernance assure la prise en charge et la surveillance des principaux risques

Opportunités d'amélioration

Les responsabilités du CAIPRP sont en train d'être redéfinies à la suite de la nouvelle mission attribuée à la DTITN. La réévaluation des responsabilités de cette direction quant à la prise en charge des incidents informatiques impliquant des RP génère de l'ambiguïté sur les responsabilités des intervenants et intervenantes.

La structure de gouvernance en gestion des risques pour assurer la prise en charge et la surveillance des principaux risques liés aux RP n'est pas encore établie : les rôles et responsabilités des parties prenantes en gestion des risques ne sont pas clairement définis ni communiqués.

RECOMMANDATIONS

4. Définir les rôles et responsabilités des principaux intervenants et intervenantes dans la gestion des risques liés aux RP. Rédiger une politique de gestion des risques et la faire approuver par le conseil municipal.
5. Évaluer périodiquement l'efficacité du cadre de gestion des incidents de PRP, et identifier et implémenter des actions correctives s'il y a lieu. Effectuer la reddition de comptes selon les paramètres définis à la recommandation 3.

Critère 3 : Les ressources allouées sont suffisantes pour que des plans d'action adéquats soient établis et mis en œuvre comme prévu.

Opportunités d'amélioration

Le modèle de gestion des risques, les outils de travail et le plan d'action de gestion des risques n'ayant pas été déterminés, les ressources nécessaires n'ont pas été déterminées de façon détaillée.

Lorsque les formations sur la PRP et l'ÉFVP ont été offertes aux gestionnaires et directeurs de la Ville, les attentes concrètes sur les actions attendues à court et moyen terme en priorisant les RP des citoyens, n'ont pas été communiquées aux participants et participantes, étant donné que les priorités n'avaient pas encore été établies en gestion des risques.

L'analyse des besoins de formation en gestion des risques n'a pas été effectuée, et aucune formation n'a été offerte à cet égard. Les employés et employées qui devront contribuer à l'analyse des risques des RP de la population ont besoin de recevoir une telle formation.

RECOMMANDATIONS

6. Effectuer l'analyse des besoins de formation en gestion des risques du personnel responsable de la gestion des risques de PRP; définir et mettre en œuvre un programme de formation pour répondre à ces besoins ainsi qu'un plan d'accompagnement et de soutien pour assurer sa mise en application.
7. Communiquer les attentes concrètes sur les actions à prendre à court et moyen terme aux personnes qui ont participé aux formations, en les informant notamment des mesures à prendre à court terme pour les RP de la population qui seront priorisés en gestion des risques.
8. Établir un budget détaillé démontrant que les ressources nécessaires sont allouées pour réaliser les actions prévues au plan d'action de gestion des risques liés aux RP, plan d'action à venir.
9. Établir les mesures disciplinaires à mettre en place pour les personnes qui seront reconnues responsables de malversation (vol, exfiltration, altération de données, etc.) et les communiquer au personnel.

Commentaire de la direction générale

La Direction générale de la Ville de Lévis accueille positivement les constats et recommandations émis dans le cadre de l'audit portant sur la gestion des risques liés à la protection des renseignements personnels.

Consciente de l'importance de cette responsabilité, la Direction générale considère la protection des renseignements personnels comme un pilier essentiel de la relation de confiance avec la population. Elle constitue également une priorité transversale qui doit accompagner l'ensemble des initiatives municipales, notamment dans le contexte de la transformation numérique.

Des actions sont déjà en cours pour renforcer la gestion des risques en la matière, et la mise en œuvre des recommandations issues de ce rapport d'audit s'inscrit dans cette démarche d'amélioration continue. La Direction générale tient à souligner le professionnalisme et la rigueur de l'équipe d'audit, qui ont permis de formuler des recommandations de grande qualité.

Annexe I - Portée et objectif de l'audit

Portée de l'audit

En vertu des dispositions de la *Loi sur les cités et villes* (RLRQ, chap. C-19), j'ai réalisé une mission d'audit de performance portant sur la gestion de la PRP à la Ville de Lévis.

Les RP couverts dans cette mission d'audit et les processus de gestion entourant leur protection incluent tous ceux que la Ville a collectés de ses citoyens et citoyennes, de son personnel et de ses fournisseurs, que ces données soient hébergées sur ses propres serveurs ou chez des fournisseurs (sur site à l'interne ou dans l'infonuagique).

Toutefois, les RP collectés directement par les instances suivantes sont exclus de la portée de l'audit :

- le Bureau de la présidente d'élection et responsable de registres et de référendums municipaux de la Ville de Lévis;
- la Cour municipale de la Ville de Lévis;
- la Direction du Service de police de la Ville de Lévis.

Ces instances exercent leurs fonctions légales sous la surveillance d'un organisme de régulation externe. Les données qu'elles collectent peuvent être assujetties à d'autres règles propres à leurs activités. Dans ce contexte, et pour que leur indépendance et leurs responsabilités soient respectées, leur processus de gestion des RP est exclu de la portée du présent audit.

Cette mission a été réalisée conformément à la Norme canadienne de missions de certification (NCMC 3001) émise par le Conseil des normes d'audit et de certification soutenu par CPA Canada.

Le présent rapport a été achevé le 2 juillet 2025.

Objectif et critères d'évaluation

La présente mission vise à assurer que la méthodologie de gestion des risques liés aux RP permet de bien identifier, évaluer et mitiger les risques de non-conformité aux exigences légales et règlementaires, en fonction de la criticité, ainsi que d'affecter les ressources nécessaires pour effectuer les travaux selon les priorités établies.

Les critères d'évaluation retenus pour cet audit sont tirés des bonnes pratiques en gestion des risques et des exigences en matière de gestion de la PRP contenues dans les lois et règlements auxquels la Ville est assujettie.

Critère d'audit 1 : La gestion des risques liés aux RP est effectuée selon une approche systématique et structurée :

1.1 Les principaux risques sont identifiés et évalués à partir d'un modèle fondé sur des référentiels reconnus et approuvé par la Direction générale;

1.2 Les menaces et vulnérabilités technologiques rendant possibles les fuites et vols d'informations sont connues et prises en compte dans l'évaluation des risques;

1.3 Le plan d'action et le calendrier de réalisation qui priorisent les interventions sont approuvés par la Direction générale;

1.4 La reddition de comptes informe des risques priorisés et de l'avancement des travaux.

Critère d'audit 2 : La structure de gouvernance assure la prise en charge et la surveillance des principaux risques :

2.1 Les rôles et responsabilités des parties prenantes sont clairement définis et communiqués;

2.2 Les politiques et directives sont conformes aux exigences de la Loi sur l'accès et diffusées adéquatement sur le site Web ou sur l'intranet selon le cas.

Critère d'audit 3 : Les ressources allouées sont suffisantes pour que des plans d'action adéquats soient établis et mis en œuvre comme prévu.

3.1 Les budgets sont suffisants pour que les outils technologiques soient acquis et déployés et pour que les ressources humaines requises soient allouées;

3.2 Les outils de travail disponibles favorisent l'opérationnalisation optimale;

3.3 La formation est planifiée selon les besoins, et la méthode d'apprentissage est adaptée au profil des personnes.

Responsabilité de la vérificatrice générale

La responsabilité de la vérificatrice générale de la Ville de Lévis consiste à fournir une conclusion sur les objectifs de l'audit, et elle peut émettre des recommandations. Pour ce faire, j'ai recueilli les éléments probants suffisants et appropriés pour fonder ma conclusion et pour obtenir un niveau d'assurance raisonnable. Mon évaluation est basée sur les critères que j'ai jugés valables dans les circonstances.

La vérificatrice générale de la Ville de Lévis applique les Normes canadiennes de gestion de la qualité (NCGQ 1 et 2) présentées dans le Manuel de CPA Canada – Certification. Ainsi, elle conçoit et maintient un système de gestion de la qualité qui comprend des normes internes documentées en ce qui concerne la conformité aux règles de déontologie, aux normes professionnelles et aux exigences légales et règlementaires applicables, et veille au bon fonctionnement de ce système. De plus, elle se conforme aux règles sur l'indépendance et aux autres règles du C*ode de déontologie des comptables professionnels agréés* du Québec, lesquelles reposent sur les principes fondamentaux d'intégrité, d'objectivité, de compétence professionnelle et de diligence, de confidentialité et de conduite professionnelle.

Annexe II - Rôles et responsabilités en matière de PRP

La Loi sur l'accès établit la gouvernance en matière d'accès aux documents et de PRP pour les organismes publics visés, dont les municipalités. À cet égard, voici les rôles et responsabilités des principaux intervenants extraits des politiques et directives de la Ville.

La personne ayant la plus haute autorité au sein de la Ville (maire)

Le ou la maire de la Ville est d'office responsable de la PRP en exerçant la fonction de responsable de la PRP[2]. Cette responsabilité a été déléguée à la personne directrice du greffe et greffière de la Ville, qui doit pouvoir l'exercer de manière autonome et assurer le respect et la mise en œuvre de la Loi sur l'accès. Après avoir délégué cette responsabilité, le ou la maire veille à faciliter l'exercice de celle-ci dans l'organisation.

Conseil municipal de la Ville

La Ville met en place les mesures raisonnables permettant à la personne responsable de l'accès aux documents et de la protection des renseignements personnels (RAPRP) et greffière d'exercer ses fonctions dans un environnement qui assure son autonomie, son indépendance et sa neutralité. De plus, la Ville s'assure de rendre disponibles toutes les ressources humaines, matérielles et financières que la personne RAPRP et greffière estime requises pour exercer ses fonctions.

Le conseil municipal de la Ville a délégué au comité exécutif l'exercice des pouvoirs qui lui sont conférés par la Loi sur l'accès[3]. Ce comité exerce donc un rôle décisionnel, notamment en matière de PRP, envers l'administration municipale.

Le comité exécutif confie au directeur général ou à la directrice générale la responsabilité de soutenir l'administration municipale dans l'application de la présente politique.

Direction générale

Le directeur général ou la directrice générale préside le CAIPRP. Il ou elle s'assure de soumettre aux instances toute demande visant la disponibilité des ressources nécessaires pour :

- Que la Ville puisse s'acquitter de ses obligations en matière de PRP;
- Effectuer la gestion des incidents de confidentialité selon leur niveau de criticité et les conséquences qu'ils peuvent avoir sur la réputation de la Ville ou la vie de la personne concernée.

[2] Article 8 de la Loi sur l'accès.

[3] Article 18, paragraphe 16 du Règlement intérieur du conseil de la Ville RV-2024-34-42.

CAIPRP

Ce comité relève du directeur général ou de la directrice générale, et son principal mandat est de soutenir la personne RAPRP et greffière de la Ville dans l'exécution de ses obligations.

Le comité peut formuler tout avis ou recommandation pour soutenir cette personne et la conseiller dans la gestion de la politique. Enfin, le comité prend connaissance du rapport de gestion que lui dépose annuellement la ou le RAPRP, qui propose notamment toute mesure pouvant optimiser et améliorer les processus de PRP pratiqués par la Ville. Le comité peut formuler tout avis et recommandation à la lumière de ce rapport, et notamment les mesures d'optimisation et d'amélioration de la protection de la vie privée et des renseignements personnels.

La personne RAPRP informe, de façon diligente, le comité de la survenance d'un incident de confidentialité des RP. Elle fait rapport régulièrement au comité de l'état de la situation dans le cadre de la gestion d'un incident de confidentialité. Le comité peut formuler tout avis ou recommandation pour la soutenir et la conseiller dans la gestion d'un tel incident. Enfin, le comité prend connaissance du rapport de gestion d'un incident de confidentialité que lui dépose la personne RAPRP et peut formuler tout avis et recommandation à la lumière de ce rapport et, de façon générale, sur la gestion d'un incident de confidentialité, dont notamment les mesures de mitigation et de suivi.

Responsable de l'accès aux documents et de la PRP

La personne directrice du greffe et greffière assume la responsabilité et exerce la fonction de RAPRP de la Ville. Elle exerce cette fonction et les pouvoirs qui lui sont délégués par le ou la maire et assume en conséquence les responsabilités qui lui sont dévolues à titre de responsable de la PRP, telles que prévues à la Loi sur l'accès. Elle traite les demandes formulées par les citoyens et citoyennes en matière de communication, de correction ou d'autres demandes relatives aux RP que l'administration municipale détient. Enfin, elle exerce un rôle-conseil auprès des directions de la Ville et assume les responsabilités qui lui sont confiées à ce titre.

Elle est responsable de la réalisation de l'ensemble des phases de la gestion :

- de la vie privée et des RP;
- d'un incident de confidentialité des RP.

Elle est responsable de la tenue des registres exigés par la Loi sur l'accès, incluant notamment le *Registre des incidents de confidentialité des renseignements personnels*.

Elle est responsable de réaliser toute ÉFVP et formule toute recommandation à ce sujet au CAIPRP et aux directeurs et directrices de la Ville.

Elle siège au CAIPRP, collabore avec la Ville, le comité exécutif, le directeur général ou la directrice générale, assume un rôle-conseil et fournit des avis et recommandations auprès de ceux-ci dans le cadre de la mise en œuvre des politiques de la Ville.

Répondant ou répondante PRP- Directions de la Ville

Le répondant ou la répondante agit comme personne de référence en matière de PRP au sein de sa direction. Cette personne :

- répond aux questions de ses collègues (premier niveau);
- soutient ses collègues dans l'identification des risques;
- propose des actions pour mitiger les risques;
- diffuse les bonnes pratiques en matière de PRP au sein de sa direction.

Gestionnaires et personnel de la Ville

L'ensemble du personnel de la Ville est responsable de mettre en œuvre les politiques et directives dans le cadre de l'exercice de leur fonction. À ce titre, tout membre du personnel de la Ville qui a un motif raisonnable de croire qu'un écart important ou un manquement grave à l'égard d'une politique a été commis ou est sur le point de l'être, en informe sans délai directement son directeur ou sa directrice, qui en informe la greffière.

Le personnel cadre et les directeurs et directrices veillent à l'application des politiques et directives auprès du personnel sous leur supervision. De plus, ils soutiennent la greffière de la Ville, lui transmettent tout avis ou recommandation appropriés et collaborent avec elle dans la mise en œuvre des politiques et directives. Ils mettent également en œuvre les mesures de prévention et de sensibilisation recommandées auprès du personnel qu'ils supervisent. Enfin, ils mettent en place toute mesure de mitigation et veillent à la mise en œuvre de toute recommandation et de toute autre mesure identifiée pour prévenir tout écart ou manquement, avec la collaboration du personnel de la Ville concerné.

La DTITN, en collaboration avec le conseiller ou la conseillère en sécurité de l'information, soutient également la greffière de la Ville et son équipe, fournit des recommandations et assume un rôle-conseil auprès d'elles, recommande à la greffière les priorités d'intervention sur le plan des technologies de l'information, suivant l'analyse des risques informatiques réalisée au préalable, et formule tout avis de sécurité dans l'application des politiques de la Ville. Elle a également la responsabilité de veiller à ce que les mesures adéquates de protection des données de la Ville aient été mises en place par les fournisseurs concernés.

Chaque directeur ou directrice est responsable de formuler une demande d'ÉFVP, de participer activement à cette évaluation et de veiller à la mise en œuvre des recommandations formulées aux termes de cette évaluation, et ce, à l'égard de chaque projet visé sous sa responsabilité.

Annexe III - Politiques et directives à la Ville de Lévis

Au fil des ans, et particulièrement depuis la sanction de la Loi 25, la Ville s'est dotée d'un cadre de gouvernance couvrant la PRP et la gestion documentaire.

Politiques et directives	Description
En matière de PRP	
Directive relative à la régie interne du comité sur l'accès à l'information et la PRP *(en cours de révision)*	Cette directive a pour objectif de déterminer le mandat et d'établir les règles de fonctionnement de ce comité.
Politique sur la gouvernance de la protection de la vie privée et des renseignements personnels.	Cette politique, adoptée par le comité exécutif : • énonce les principes encadrant la gouvernance de la Ville à l'égard de la vie privée et des RP, tout au long de leur cycle de vie, et ceux encadrant l'exercice des droits des personnes concernées; • prévoit le processus de traitement des plaintes relatives à la PRP; • définit les rôles et responsabilités en matière de PRP à la Ville; • décrit les activités de formation et de sensibilisation que la Ville offre à son personnel.
Politique sur la confidentialité des renseignements personnels recueillis par un moyen technologique.	Cette politique, adoptée par le comité exécutif, a pour objectif : • d'énoncer les orientations et les principes directeurs destinés à assurer efficacement la confidentialité de tout RP collecté par tout moyen technologique; • de protéger la confidentialité de tout RP collecté par la Ville tout au long de son cycle de vie; • d'indiquer les moyens technologiques utilisés pour collecter tout RP, les fins auxquelles il est collecté et son traitement par la Ville; • d'assurer la confiance du public à l'égard de la Ville en faisant preuve de transparence concernant le traitement des RP et les mesures de protection et d'accès qui les encadrent.
Directive sur la gestion des incidents de confidentialité des renseignements personnels.	Cette directive établit le processus applicable à la gestion des incidents de confidentialité des RP détenus par la Ville dans le cadre de la réalisation de ses activités, ainsi que les rôles et responsabilités des principaux intervenants et intervenantes lors de la mise en œuvre de ce processus.
Directive sur la gestion d'une évaluation des facteurs relatifs à la vie privée	Cette directive précise les situations dans les projets ou les initiatives impliquant des RP où la Loi sur l'accès prévoit que la Ville doit procéder à une ÉFVP.
Directive sur les sondages *(en cours de préparation)*	Cette directive établira les exigences quant à la PRP lors des sondages impliquant la collecte ou la communication de RP, réalisés par la Ville ou un de ses mandataires.

Politiques, directives et procédures	Description
En matière de la sécurité de l'information	
Politique d'utilisation des actifs informationnels.	Cette directive a pour objectif : • d'informer les utilisatrices et utilisateurs des règles et des modalités régissant l'utilisation des actifs informationnels; • de définir les droits, les obligations et les responsabilités des utilisateurs et utilisatrices dans l'utilisation des actifs informationnels; • d'aviser les utilisatrices et utilisateurs de l'existence de certaines mesures de contrôle quant à l'utilisation qui en est faite; • de sensibiliser les utilisatrices et utilisateurs sur les conséquences découlant d'une utilisation inappropriée et/ou illégale des actifs informationnels.
Directive sur la gestion des codes d'accès et des mots de passe.	Cette directive vise à assurer l'intégrité, la confidentialité, la disponibilité de l'information et la protection des actifs informationnels appartenant à la Ville. Elle définit : • les règles concernant les codes d'accès et les mots de passe; • les responsabilités et l'imputabilité des parties prenantes; • les règles au regard du comportement des utilisateurs, afin que ceux-ci contribuent également à la gestion sécuritaire des actifs informationnels.
Directive sur l'acquisition ou la modification de systèmes ou de services en technologies de l'information.	Cette directive vise à assurer une compréhension et des actions appropriées pour atteindre les objectifs suivants : • une approche structurée d'acquisition de systèmes et services en technologies de l'information; • l'intégrité de l'information; • la protection des RP; • l'optimisation des investissements en technologies de l'information; • l'ouverture à l'utilisation de systèmes modernes et performants.
Politique de sécurité de l'information *(en cours de préparation)*	La politique de sécurité de l'information est un ensemble de lignes directrices et de principes auxquels une organisation adhère pour protéger ses actifs informationnels, réduire les risques d'incidents de sécurité et assurer la confidentialité, l'intégrité et la disponibilité de ses données. Elle établit un cadre global pour la gestion de la sécurité de l'information au sein de l'organisation. Elle définit clairement les rôles et responsabilités ainsi que les objectifs de sécurité, incluant la traçabilité ou la capacité à retracer toutes les actions effectuées sur les systèmes d'information.

Politiques, directives et procédures	Description
En matière de gestion documentaire	
Politique de gestion documentaire.	Cinq objectifs généraux permettent d'assurer la mise en œuvre de cette politique : • Favoriser l'implication du personnel à l'égard de l'application des procédures de gestion documentaire qui découlent de la présente politique; • Établir un cadre de gestion uniforme favorisant les moyens et les ressources les plus efficaces et les plus rentables pour créer, recevoir, identifier, organiser, enregistrer, repérer, diffuser, reproduire, protéger, conserver et éliminer les documents de la Ville; • Favoriser l'accès aux documents et soutenir la protection des renseignements personnels détenus par la Ville dans l'exercice de ses fonctions; • Assurer la protection des documents ayant une valeur administrative, légale, financière ou historique; • Assurer la préservation des documents essentiels et de la mémoire organisationnelle de la Ville de Lévis.
Règle de conservation	*Loi sur les archives* (RLRQ, c. A-21.1)
Plan de classification 2023	Le plan de classification est un outil qui détermine la structure logique et hiérarchique permettant le regroupement intellectuel des fonctions et des activités de la Ville. Il s'agit d'un outil complémentaire au calendrier de conservation : le calendrier indique les délais de conservation des documents composant un dossier, alors que le plan de classification indique l'ordre de classement des dossiers.

Annexe IV - Catégories de renseignements personnels

Le gouvernement du Québec regroupe les RP en 6 catégories pour faciliter la sensibilisation. Ces catégories sont les suivantes[4] :

Renseignements d'identification

Adresse, numéro de téléphone, sexe, âge, numéro d'assurance sociale, numéro d'assurance maladie, identifiant numérique, etc.

Renseignements de santé

Dossier médical, diagnostic, consultation d'une professionnelle ou d'un professionnel de la santé, médicament, ordonnance, cause d'un décès, etc.

Renseignements financiers

Revenu d'une personne, renseignements relatifs à l'impôt, numéro de compte bancaire, biens possédés, numéro de carte de crédit, etc.

Renseignements relatifs au travail

Dossier disciplinaire, motifs d'absence, dates de vacances, salaire, évaluation du rendement, heures d'entrée et de sortie liées au lieu de travail, etc.

Renseignements scolaires et relatifs à la formation

Inscription et choix de cours, résultats scolaires, diplômes, curriculum vitæ, etc..

Renseignements relatifs à la situation sociale ou familiale

Documents qui attestent l'état civil, le fait qu'une personne ait ou non des enfants ou qu'elle reçoive des prestations d'aide sociale ou de chômage, etc.

Les RP suivants doivent généralement être considérés comme sensibles : financiers, génétiques ou biométriques, concernant la santé, la vie sexuelle ou l'orientation sexuelle, les convictions religieuses ou philosophiques, les opinions politiques ainsi que l'origine ethnique ou raciale.

[4] Voir la Présentation des concepts-clés liés aux renseignements personnels *Présentation des concepts-clés liés aux renseignements personnels | Gouvernement du Québec*

Contrôles généraux informatiques

Audit de performance

CHAPITRE 3

Lévis | VÉRIFICATEUR GÉNÉRAL

3

Contrôles généraux informatiques
Audit de performance

Table des matières

Liste des acronymes

CGI	Contrôles généraux informatiques
COBIT	Objectifs de contrôle de l'information et des technologies associées (Control Objectives for Information and Related Technology)
DFIN	Direction des finances et de la trésorerie
DTITN	Direction des technologies de l'information et de la transformation numérique
MEP	Mise en production
NCA	Normes canadiennes d'audit
SSO	Solution d'authentification unique (Single Sign On)
TI	Technologie de l'information
Unit4	U4, Progiciel de gestion intégrée

Contexte

La *Loi sur les cités et villes*[1] exige que les états financiers annuels d'une municipalité soient audités par un cabinet indépendant ou par le vérificateur général de cette municipalité, selon la décision de ce dernier. La firme Mallette S.E.N.C.R.L. (ci-après « Mallette ») a été mandatée pour effectuer l'audit des états financiers des années 2022, 2023 et 2024 de la Ville de Lévis (ci-après « la Ville »).

La préparation des états financiers de la Ville repose en grande partie sur l'utilisation de systèmes informatiques incluant des logiciels financiers et leurs bases de données, ainsi que les composantes nécessaires à leur fonctionnement (système d'exploitation, réseau et unités de stockage).

À la Ville, un grand volume de données est traité par les applications informatiques, et beaucoup de transactions sont déclenchées et enregistrées automatiquement. Le trésorier s'appuie largement sur des contrôles intégrés à des applications informatiques dont l'efficacité du fonctionnement dépend notamment des contrôles généraux informatiques (CGI). L'utilisation de l'informatique, bien qu'incontournable, apporte un risque sur le plan de l'intégrité[2] de l'information utilisée dans la gestion quotidienne et dans la préparation des états financiers. Dans ce contexte, les CGI sont essentiels pour assurer le fonctionnement systématique et efficace des contrôles qui dépendent des systèmes informatiques.

Les CGI assurent le fonctionnement systématique et efficace des contrôles qui dépendent des systèmes informatiques.

La vérificatrice générale a jugé approprié de réaliser l'audit des contrôles généraux informatiques pour l'année 2024. Cette mission a aussi permis d'examiner les principales pratiques de gestion des risques de cybermenace mises en œuvre par la Direction des technologies de l'information et de la transformation numérique (DTITN) de la Ville. Notons que, depuis 2021, plusieurs municipalités du Québec ont été victimes d'attaques qui ont provoqué des pannes des services informatiques importantes, voire majeures.

À cet égard, le magazine *Scribe,* de la Fédération québécoise des municipalités, a publié un article en novembre 2023 intitulé « *Serez-vous la prochaine municipalité victime d'une cyberattaque?* ». L'auteur y mentionne : « *Tous les experts s'entendent sur le fait qu'en cybersécurité, l'axe d'analyse du risque n'est pas de savoir si l'on va être attaqué, mais plutôt quand.* » En octobre 2024, le Centre canadien pour la cybersécurité confirme dans son rapport que les cybermenaces complexes sont en pleine expansion au Canada.

[1] Articles 107.7 ainsi que 108 à 108.6 de la LCV.

[2] Exactitude, …, exhaustivité, validité (NCA 315, par.12, A6, A148 et A 149).

Objectif et portée de l'audit

Notre premier objectif est d'évaluer l'efficacité du fonctionnement des 26 CGI sur lesquels Mallette a choisi de s'appuyer dans sa stratégie d'audit des états financiers (annexe IV). Nous avons évalué ces CGI tout au long de l'année 2024. Parmi ces contrôles, cinq ont été audités pour la première fois.

Les procédures d'audit sont effectuées pour chaque aspect de l'environnement informatique suivant :

i. Logiciels Unit4

ii. Logiciels de gestion de bases de données

iii. Logiciels de bases (systèmes d'exploitation, réseau, Virtualisation, pilotes de périphériques, pare-feu et logiciel de communication)

Dans le cadre d'un audit des états financiers, la vérificatrice ou le vérificateur se concentre sur le fonctionnement des contrôles pour détecter, prévenir et corriger les erreurs en vue d'assurer l'intégrité des informations. Toutefois, notre audit apporte aussi un regard indépendant sur les risques de fraude internes et externes que certains CGI audités, du fait de leur nature, permettent de réduire.

Finalement, notre mandat fournit à la DTITN et à la direction des finances et de la trésorerie (DFIN) des constatations et recommandations pour améliorer le contrôle interne. Nous avons aussi rencontré les membres du comité des finances de la Ville pour discuter des résultats de notre audit.

Les CGI ne peuvent éliminer le risque de fraude ni garantir l'intégrité de l'information financière dans les systèmes de la Ville. Mais il est essentiel que le contrôle interne soit conçu pour fournir une assurance raisonnable de la qualité de l'information financière.

Système de contrôle interne pour l'information financière

Le paragraphe 18 de l'annexe 5 de la norme NCA 315 précise que les risques découlant du recours à l'informatique sur la fiabilité des états financiers comprennent notamment les risques associés à un appui inapproprié sur des applications informatiques qui ne traitent pas les données avec exactitude, qui traitent des données inexactes, ou les deux. Voici des exemples de ces risques :

- Accès non autorisé aux données pouvant aboutir à des destructions ou modifications inappropriées de données, y compris l'enregistrement d'opérations non autorisées ou inexistantes ou l'enregistrement inexact d'opérations. L'accès de multiples utilisateurs à une base de données commune peut poser des risques particuliers;
- Possibilité que le personnel du service informatique obtienne des privilèges d'accès supérieurs à ceux qui sont nécessaires pour l'exercice de ses fonctions, et que la séparation des tâches se trouve ainsi compromise;
- Modifications non autorisées des données dans les fichiers maîtres;
- Modifications non autorisées d'applications informatiques ou d'autres aspects de l'environnement informatique;
- Non-réalisation de modifications nécessaires d'applications informatiques ou d'autres aspects de l'environnement informatique;
- Interventions manuelles inappropriées;
- Perte possible de données ou incapacité d'accéder aux données requises.

Rôle des CGI dans la fiabilité de l'information financière

Les CGI contribuent à assurer le bon fonctionnement continu de l'environnement informatique, notamment le maintien du fonctionnement efficace des contrôles du traitement de l'information et l'intégrité (c'est-à-dire l'exhaustivité, l'exactitude et la validité) des informations se trouvant dans le système d'information de l'entité. Nous avons audité les CGI importants des trois catégories suivantes :

Gestion des accès

Maintenir un degré de contre-pouvoir approprié exige que plus d'une personne participe à la réalisation d'une transaction.

La gestion des accès vise à assurer que les accès sont octroyés uniquement aux utilisatrices et utilisateurs de systèmes autorisés pour créer des transactions financières, les autoriser ou les enregistrer et que ces accès sont appropriés et sécurisés. Ce mode de fonctionnement permet aussi de protéger les actifs de la Ville.

Une gestion optimale des accès applique le principe du moindre privilège, qui consiste à accorder à une personne utilisatrice uniquement les permissions nécessaires à l'accomplissement de ses tâches, en fonction des rôles, des responsabilités et des besoins. Cela facilite une bonne séparation des tâches, un degré de contre-pouvoir approprié en exigeant que plus d'une personne participe à la réalisation d'une transaction. La probabilité d'erreur ou de fraude diminue considérablement lorsqu'au moins deux personnes participent activement au traitement d'une transaction. La fraude intentionnelle devient difficile à réaliser, car elle exige une collusion entre deux personnes ou plus. Elle dissuade les fraudeurs, qui savent que leurs actions ne passeront probablement pas inaperçues.

Gestion des changements

La gestion des changements vise à assurer que les modifications apportées aux systèmes d'information, aux applications et aux infrastructures sont effectuées de manière contrôlée et sécurisée. Elle minimise les risques associés aux changements et fait que ces derniers sont réalisés de manière efficace et ne perturbent pas les opérations normales.

Encadre les modifications apportées aux systèmes de manière contrôlée et sécurisée.

Le processus de gestion des changements encadre toutes les modifications des applications et de leurs bases de données, des interfaces et des agents intelligents (Intel Agent), des logiciels de base ainsi que des équipements informatiques. Il vise aussi les modifications de la paramétrisation et la mise en place des correctifs de sécurité.

Toute modification importante doit être soumise à un processus structuré de gestion des changements. Cela implique les actions suivantes :

- Évaluer les risques associés aux changements et définir les tests nécessaires;
- Faire approuver les changements par les parties prenantes appropriées;
- Contrôler la mise en œuvre des changements.

Gestion des opérations

Surveille les points vulnérables de l'environnement informatique.

La gestion des opérations vise à assurer que les processus informatiques sont exécutés de manière stable, efficace et conforme aux exigences de l'organisation, tout en minimisant les interruptions et en optimisant l'utilisation des ressources. Elle comprend également la mise en place de contrôles pour assurer la surveillance des points vulnérables de l'environnement informatique ou le suivi des intrusions dont il fait l'objet.

Voici les cinq composantes du contrôle interne qui dépendent de l'efficacité du fonctionnement des CGI :

i) Environnement de contrôle

La Direction générale a développé et entretient une culture organisationnelle d'honnêteté et de comportement éthique.

ii) Évaluation des risques

La DTITN et la DFIN évaluent les risques pertinents pour la préparation des états financiers lors de la création du système de contrôle interne et lors de la revue périodique de ce système.

iii) Activités de contrôle

Les activités de contrôle aident à s'assurer que les directives de gestion sont mises en œuvre et que les risques liés à la préparation des états financiers sont maîtrisés.

iv) Système d'information et communications

Le système d'information et les communications de l'entité contribuent adéquatement à la préparation de ses états financiers.

v) Suivi

Le suivi du système de contrôle interne par la DTITN et la DFIN assure que tout fonctionne comme prévu.

Les CGI sont essentiels pour assurer le fonctionnement de tous les contrôles qui dépendent des systèmes informatiques. En d'autres mots, les contrôles financiers dépendent des CGI comme la solidité d'un édifice dépend de ses fondations.

Les contrôles financiers dépendent des CGI comme la solidité d'un édifice dépend de ses fondations.

Résultats de l'audit

Conformément aux normes NCA 260 et 265, une lettre contenant les résultats détaillés de notre audit a été transmise à la DTITN et à la DFIN. Nous avons aussi rencontré les membres du comité des finances de la Ville pour discuter des résultats de notre audit. Cette lettre, comme c'est la pratique pour les communications adressées aux responsables de la gouvernance, est confidentielle. Le résultat du suivi effectué par la vérificatrice générale concernant les recommandations émises sera aussi confidentiel.

Dans le même ordre d'idées, notre évaluation des 26 contrôles audités a été retirée de l'extrait du rapport d'audit dans le tableau présenté dans la section « Sommaire de l'évaluation des CGI sélectionnés ».

Il serait inapproprié de communiquer notre évaluation de l'efficacité du fonctionnement des contrôles à la Ville au cours de 2024, mais nous sommes en mesure d'affirmer qu'un niveau d'efficacité élevé a été démontré pour plusieurs d'entre eux.

Notons par ailleurs que, bien que les ressources internes en sécurité informatique soient très limitées, la Municipalité a fait appel à des entreprises qualifiées pour bénéficier de compétences élargies sur les aspects de la cybersécurité. Grâce à ces partenaires, la Ville a accès à des outils et services de surveillance 24/7 pour déceler des activités suspectes dans ses systèmes. Les services incluent des logiciels de protection pouvant être mis à jour en continu ainsi que des tests d'intrusion.

Lettre transmise à la DTITN et à la DFIN de la Ville

Voici un extrait des recommandations transmises à la DTITN et à la DFIN :

Gouvernance

Nous recommandons de désigner une personne responsable de la gouvernance des CGI pour coordonner les travaux des directions impliquées. Les principales tâches que la personne responsable des CGI doit accomplir, personnellement ou par l'intermédiaire de ses collaboratrices et collaborateurs des diverses directions, sont les suivantes (notez qu'à la Ville, certaines de ces tâches sont déjà prise en charge, en totalité ou en partie, par divers employés des opérations TI) :

1° Évaluation des risques

- Identifier les risques informatiques concernant les vulnérabilités et déficiences internes ainsi que les menaces externes.
- Évaluer les risques concernant l'intégrité, la confidentialité et la disponibilité des informations critiques, ainsi que la traçabilité des actions des utilisatrices et utilisateurs, en prenant en compte les risques d'erreur et de fraude.
- Définir la tolérance au risque pour l'information financière et pour les autres informations critiques. Lorsque la cible n'est pas un risque résiduel faible, elle doit être approuvée par la Direction générale.
- Réaliser des tests d'efficacité des contrôles existants (tests d'intrusion[3], simulations de cyberattaques[4], tests de récupération après sinistre, etc.).
- Analyser les vulnérabilités soulevées et les pistes de solutions proposées dans les rapports des tests d'intrusion. Prioriser les actions de remédiation selon la tolérance aux risques, définir un calendrier d'intervention et en faire le suivi.

2° Conception et mise en place des contrôles

- Concevoir et mettre en place des contrôles pour protéger les systèmes d'information, l'intégrité, la disponibilité et la confidentialité des données ainsi que la traçabilité des actions.
- S'assurer que le portefeuille de contrôles couvre toutes les applications financières importantes, selon l'évaluation des risques. Privilégier la stratégie de mitigation préventive plutôt que détective[5] tout en considérant l'efficacité opérationnelle et l'optimisation des coûts.

[3] Identifier les vulnérabilités techniques dans les systèmes.

[4] Tester la préparation organisationnelle face à une cyberattaque réelle (évaluer la capacité de détection et de réponse des équipes de sécurité aux incidents de cybersécurité; analyser les processus de gestion des incidents et de communication en situation de crise; former et sensibiliser le personnel pour qu'il réagisse efficacement en cas d'attaque réelle).

[5] Contrôles préventifs : ils visent à éviter que des problèmes se produisent. Ces contrôles sont conçus pour réduire le risque d'incidents en limitant les possibilités d'erreur ou de fraude.
Contrôles détectifs : ils ont pour but de détecter les erreurs ou fraudes après qu'elles sont déjà matérialisées, préférablement dès qu'elles se produisent. Ces contrôles incluent des activités telles que la réconciliation, la révision, le décompte des actifs et les audits.

3° Politiques, directives, procédures

- Définir les pièces de gouvernance nécessaires à l'encadrement des ressources (personnel et consultantes et consultants) et en assurer la communication.
- S'assurer que ces documents sont maintenus à jour selon les exigences légales, les nouvelles menaces, les vulnérabilités découvertes ou les changements dans l'environnement technologique de l'organisation.

4° Communications avec les auditeurs externes

- Prendre contact avec les auditeurs externes pour comprendre les CGI sur lesquels ils comptent s'appuyer et les évidences requises pour démontrer l'application efficace tout au long de l'année. Définir les règles de séparation des tâches importantes pour l'auditeur.
- Définir les logiciels et équipements informatiques inclus dans la portée des travaux des auditeurs externes.

5° Formation et sensibilisation

- Informer les gestionnaires et le personnel sur les attentes liées aux CGI dont ils ont la responsabilité : application conforme tout au long de l'année; communication immédiate de toute anomalie; interdiction de modification sans autorisation préalable.
- Établir un plan pour sensibiliser le personnel aux risques d'hameçonnage et mener des campagnes de simulation d'hameçonnage afin d'évaluer la vigilance des utilisateurs et utilisatrices.

6° Amélioration continue

- Maintenir un registre des recommandations émises par les auditeurs et les fournisseurs externes.
- Prioriser les actions de remédiation et établir un calendrier d'intervention selon la tolérance aux risques.
- Effectuer une reddition de comptes à la Direction générale sur l'état des contrôles généraux informatiques, les risques identifiés et les mesures prises.
- Mettre à jour l'évaluation des risques selon les nouvelles menaces, les vulnérabilités et les changements dans l'environnement de la Ville.

Gestion des accès

Accès limité aux bases de données de Unit4

Nous recommandons d'activer la journalisation des accès pour Unit4 ainsi que ses bases de données, et de sauvegarder cette journalisation de manière qu'elle soit inaltérable. Conserver l'historique des accès octroyés et retirés au cours de l'année.

Séparation des tâches et accès incompatibles dans Unit4

Nous recommandons de documenter les règles[6] de séparation des tâches à respecter pour les accès dans Unit4 (approbation, enregistrement, garde des actifs). Modifier la paramétrisation des billetteries pour exiger l'approbation des gestionnaires dans l'octroi de privilèges exceptionnels.

Révision annuelle des accès (Unit4 / environnement TI)

Nous recommandons de mettre en place un processus de révision périodique des accès afin d'assurer le respect du principe du moindre privilège et des règles de séparation de tâches.

Gestion des changements

Restriction et séparation des tâches pour les mises en production

Nous recommandons d'établir des critères pour évaluer l'impact du changement et le classifier selon sa criticité, et de compléter le guide opérationnel pour indiquer les exigences, selon le niveau de risque, quant à :

- La documentation des changements et des tests applicables (fonctionnalité, performance, compatibilité, acceptation utilisateur, régression, etc.);
- L'approbation des utilisatrices et utilisateurs ou des gestionnaires TI ainsi que la documentation des preuves de cette approbation;
- La validation requise après la mise en production;
- La séparation des tâches entre la personne qui crée un changement et celle qui fait la mise en production.

Nous recommandons aussi de conserver l'agenda des rencontres du comité consultatif des changements.

[6] Aucune transaction ni chaîne de transactions ne doit être laissée sous la responsabilité d'une seule personne.

Sommaire de l'évaluation des CGI sélectionnés

Contrôles généraux informatiques		Efficacité du fonctionnement du contrôle[7] (Faible Moyenne Élevée)
Processus de gestion des accès		
A1	Accès limité aux bases de données de Unit4	
A2	Privilèges d'accès octroyés sont approuvés (Unit4 / environnement TI)	
A3	Révocation des accès en temps opportun (Active Directory et Unit4)	
A4	Révision annuelle des accès (Unit4 / environnement TI)	
A5	Séparation des tâches et accès incompatibles dans Unit4	
A6a	Accès à hauts privilèges dans Unit4 limités aux utilisateurs autorisés	
A6b	Octroi et surveillance des accès hauts privilèges TI	
A7	Sécurité d'authentification pour accéder aux systèmes	
A8	Attributs clés des paramètres de sécurité dans Unit4	
A9	Accès physique limité - salle des serveurs	
A10	Accès physique limité - copies de sauvegarde	
Processus de gestion des changements		
B1	Tests sur l'application Unit4 avant MEP	
B2a	Restriction pour les MEP (Unit4 et des logiciels de base)	
B2b	Séparation des tâches pour les MEP (Unit4 et logiciels de base)	
B3	Tests sur les bases de données de Unit4 avant MEP	
B4	Tests sur les logiciels de base avant MEP	
B5	Validation des changements urgents (Unit4 et logiciels de base)	
B6	Formation du personnel TI	

[7] L'évaluation a été faite pour la prévention, la détection et la correction d'erreurs aux informations financières traitées par Unit4 et utilisées pour dresser les états financiers de la Ville de Lévis en 2024, et non à l'égard du risque de fraudes.

Sommaire de l'évaluation des CGI sélectionnés

Contrôles généraux informatiques		Efficacité du fonctionnement du contrôle[7] (Faible Moyenne Élevée)
Processus de gestion des opérations		
C1	Sécurité d'authentification pour accéder au réseau	
C2	Segmentation réseau des applications Web	
C3	Analyse périodique des vulnérabilités et investigation	
C4	Surveillance et investigation des alertes générées	
C5	Contrôle d'accès VPN restreint (utilisateurs autorisés)	
C6	Sauvegarde des données financières	
C7	Contrôle d'accès pour l'exécution de travaux en lots	
C8	Suivi et correction des erreurs (intégralité du traitement)	
C9	Logiciels anti-virus	
C10	Les correctifs de sécurité sont à jour	

Commentaires de la Direction générale de la Ville

La Direction générale de la Ville de Lévis prend acte des constats formulés par la vérificatrice générale en lien avec les contrôles généraux informatiques (CGI), et en accepte les conclusions. Nous sommes déterminés à améliorer les processus de l'organisation, notamment afin d'assurer la performance de celle-ci mais également de réduire les risques dans ses opérations financières courantes. Les équipes concernées sont d'ailleurs déjà en action, de façon structurée, pour mettre en œuvre les recommandations du présent rapport d'audit.

La Direction générale tient à remercier l'équipe d'audit pour la rigueur de son travail et la qualité des recommandations formulées.

Annexe I – Objectif de l'audit et critères d'évaluation

Objectif 1 : Les CGI sélectionnés ont été mis en place pour assurer la prévention, la détection et la correction d'erreurs aux informations financières traitées par Unit4 et utilisées pour dresser les états financiers de la Ville en 2024.

> **Critère d'évaluation :** La mise en place des CGI sélectionnés a été évaluée selon la description définie par Mallette ainsi que selon le cadre de référence COBIT à l'égard des composantes de l'environnement informatique ciblées par Mallette (annexe III).

Objectif 2 : Les CGI sélectionnés ont fonctionné efficacement pour assurer la prévention, la détection et la correction d'erreurs aux informations financières traitées par Unit4 et utilisées pour dresser les états financiers de la Ville en 2024.

> **Critère d'évaluation :** Le fonctionnement efficace des CGI sélectionnés a été évalué quant à l'exécution du contrôle au cours de 2024 conformément à sa description, selon l'échelle définie par Mallette, et ce, à l'égard des composantes de l'environnement informatique ciblées par Mallette (annexe III).

Nous avons effectué notre mission d'assurance raisonnable conformément aux Normes canadiennes de missions de certification (NCMC) du *Manuel de CPA Canada – Certification*, notamment à la Norme sur les missions d'appréciation directe (NCMC 3001). L'assurance raisonnable correspond à un niveau élevé d'assurance, qui ne garantit toutefois pas qu'une mission réalisée conformément aux normes permettra de détecter toute anomalie importante à l'égard des objectifs d'audit. Les anomalies sont considérées comme importantes lorsqu'il est raisonnable de s'attendre à ce que, individuellement ou collectivement, elles puissent influer sur les décisions des utilisateurs de notre rapport.

Nous nous sommes conformés aux règles et au code de déontologie pertinents applicables à l'exercice de l'expertise comptable et se rapportant aux missions de certification 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.

La vérificatrice générale de la Ville applique les Normes canadiennes de gestion de la qualité (NCGQ 1 et 2) du *Manuel de CPA Canada – Certification*. Ainsi, elle conçoit et maintient un système de gestion de la qualité qui comprend des procédures internes documentées en ce qui concerne la conformité aux règles de déontologie, aux normes professionnelles et aux exigences légales et réglementaires applicables, et veille au bon fonctionnement de ce système. Au cours de ses travaux, la vérificatrice générale se conforme aux règles sur l'indépendance et aux autres règles prévues dans son code de déontologie, lesquelles reposent sur les principes fondamentaux d'intégrité, d'objectivité, de compétence professionnelle et de diligence, de confidentialité et de conduite professionnelle.

Annexe II – Rôles et responsabilités

Mallette est responsable de définir les contrôles généraux informatiques qui font l'objet de cet audit (ci-après « les CGI sélectionnés »). Elle est aussi responsable d'identifier les composantes de l'environnement informatique nécessaires au cheminement des opérations et au traitement de l'information financière sur lesquelles elle s'appuie dans sa stratégie d'audit.

La DTITN et la DFIN sont responsable de concevoir et de mettre en place les CGI ainsi que d'assurer l'efficacité de leur fonctionnement pour assurer l'intégrité de l'information financière.

Notre responsabilité consiste à exprimer une conclusion sur les objectifs d'audit sur la base des éléments probants obtenus pour les CGI sélectionnés. Notre évaluation est basée sur les critères décrits à l'annexe 1, que nous avons jugés valables dans les circonstances.

Nous avons recueilli les éléments probants suffisants et appropriés pour fonder nos conclusions et pour obtenir un niveau d'assurance raisonnable. La nature, le calendrier et l'étendue des procédures choisies relèvent de notre jugement professionnel.

Nos travaux d'audit ont été effectués au cours des mois de février à avril 2025 et concernent l'année financière 2024.

Annexe III – Composantes de l'environnement informatique

Les composantes de l'environnement informatique nécessaires au traitement de l'information financière incluses dans la portée de l'audit, ciblées par Mallette, sont décrites dans le tableau suivant :

APPLICATION[8]	GRAND PROCESSUS	FABRICANT / SUPPORT	BASE DE DONNÉES / SERVEUR	EMPLACEMENT
U4	Comptabilité, approvisionnement, paiements, gestion budgétaire et production de divers rapports financiers			
Systèmes d'exploitation	Logiciel de base			
Logiciels de gestion de bases de données	Logiciel de base			
Logiciels de virtualisation	Logiciel de base			
Logiciels de réseau et de communication	Logiciel de base			
Pilotes de périphériques	Logiciel de base			
Pare-feu	Logiciel de base			

[8] Aucune interface car les composantes de l'environnement informatique nécessaires au cheminement des opérations et au traitement de l'information financière incluses dans la portée de l'audit concernent seulement Unit4 et les logiciels de base.

Annexe IV – Liste des CGI sélectionnés

Les contrôles de gestion des accès suivants ont été audités :

A1 – Accès limité aux bases de données de Unit4

L'accès direct aux données inclus dans les bases de données de Unit4, c'est-à-dire sans passer par l'application Unit4, est limité aux utilisateurs autorisés de la DTITN en fonction des responsabilités et du rôle qui leur incombent. Cet accès est approuvé par la DTITN responsable du maintien des bases de données.

A2 – Privilèges d'accès octroyés approuvés (Unit4 / environnement TI)

La nature et l'étendue des privilèges d'accès modifiés ou nouvellement attribués sont approuvées par la DTITN et la DFIN, notamment en ce qui concerne les opérations donnant lieu à des informations financières critiques et à la séparation de tâches.

A3 – Révocation des accès en temps opportun (Active Directory et Unit4)

Les droits d'accès sont rapidement révoqués ou modifiés en cas de cessation d'emploi ou de mutation de l'utilisateur.

A4 – Révision périodique des accès (Unit4 / environnement TI)

Les accès utilisateurs dans Unit4 et dans l'environnement TI font l'objet d'un examen annuel pour identifier ceux qui n'ont pas été supprimés au départ d'un membre du personnel ou lors de conflits de séparation de tâches.

A5 – Séparation des tâches et accès incompatibles dans Unit4

La séparation des tâches fait l'objet d'un suivi, et les droits d'accès incompatibles sont soit abolis, soit mis en correspondance avec des contrôles d'atténuation des risques consignés par écrit et testés.

A6a – Accès à haut privilège dans Unit4 limité aux utilisateurs autorisés

Les accès à haut privilège dans Unit4 sont strictement attribués aux personnes autorisées.

A6b – Octroi et surveillance des accès à haut privilège TI

Les accès à haut privilège dans l'environnement TI (Unit4 et ses bases de données, système d'exploitation et réseau) sont accordés au besoin seulement. L'activité des comptes à haut privilège, y compris celle des administrateurs (membres du personnel et consultantes ou consultants TI) est journalisée et régulièrement surveillée.

A7 – Sécurité de l'authentification pour accéder aux systèmes

Pour accéder aux systèmes, les utilisateurs doivent s'authentifier au moyen d'un code et d'un mot de passe uniques. Les paramètres des mots de passe répondent aux bonnes pratiques (longueur minimale et niveau de complexité exigés, date d'expiration, verrouillage du compte, etc.). La sécurité multifacteur (MFA) gère les accès à distance.

A8 – Attributs clés des paramètres de sécurité dans Unit4

Les attributs clés des paramètres de sécurité sont mis en place de façon appropriée. C'est-à-dire que le système est restrictif par défaut et que des permissions doivent être attribuées pour permettre les accès en fonction des besoins seulement.

A9 – Accès physique limité - salle des serveurs

Les accès physiques aux actifs informatiques (serveurs et autres composantes) sont limités aux employées et employés TI qui en ont besoin et sont contrôlés.

A10 – Accès physique limité - copies de sauvegarde

Les accès physiques aux copies de sauvegarde sont limités aux employées et employés TI qui en ont besoin et sont contrôlés.

Les contrôles de gestion des changements suivants ont été audités :

B1 – Test sur l'application Unit4 avant MEP

Les modifications apportées à Unit4 sont rigoureusement testées et approuvées avant d'être intégrées à l'environnement de production.

B2 – Restriction et séparation des tâches pour les MEP

La possibilité d'intégrer des changements à l'environnement de production des applications (Unit4 et logiciels de base) est rigoureusement restreinte, et il y a séparation des tâches avec l'environnement de développement.

B3 – Tests sur les bases de données de Unit4 avant MEP

Les modifications apportées aux bases de données sont rigoureusement testées et approuvées avant d'être intégrées à l'environnement de production.

B4 – Tests sur les logiciels de base avant MEP

Les modifications apportées aux logiciels de base sont rigoureusement testées et approuvées avant d'être intégrées à l'environnement de production.

B5 – Validation des changements urgents (Unit4 et logiciels de base)

Les changements urgents aux logiciels de base, à Unit4 et à ses bases de données sont testés avant la mise en production ou révisés et testés après la MEP.

B6 – Formation du personnel TI

Le personnel TI reçoit la formation pour être au fait des nouveautés et connaitre les bonnes pratiques de sécurité.

Les contrôles de gestion des opérations suivants ont été audités :

C1 – Sécurité de l'authentification pour accéder au réseau

Pour accéder au réseau, les utilisateurs doivent s'authentifier au moyen de codes d'utilisateur et de mots de passe uniques ou d'autres mécanismes de validation des droits d'accès. Les paramètres des mots de passe répondent aux normes et aux politiques de l'entreprise ou de la profession.

C2 – Segmentation réseau des applications Web

Le réseau est segmenté de manière à isoler les applications Web du réseau interne, où s'effectue l'accès à Unit4.

C3 – Analyse périodique des vulnérabilités et investigation

Les gestionnaires du réseau effectuent périodiquement des analyses de vulnérabilité du périmètre du réseau et procèdent à des investigations quant aux vulnérabilités potentielles.

C4 – Surveillance et investigation des alertes générées

Des alertes sont générées pour signaler les menaces relevées par les systèmes de détection des intrusions. Les gestionnaires du réseau procèdent à des investigations au sujet de ces menaces.

C5 – Contrôle d'accès VPN restreint (utilisateurs autorisés)

Des contrôles sont en place pour restreindre l'accès au réseau privé virtuel (RPV) aux seuls utilisateurs autorisés et appropriés.

C6 – Sauvegardes des données financières

Les données financières sont sauvegardées régulièrement selon un calendrier et une fréquence établis.

C7 – Contrôle d'exécution de traitements par lots

Seules les tâches exécutées par lots par un IntellAgent testé et approuvé sont incluses dans le planificateur de lots (batch scheduler). Les autres tâches exécutées par lots sont natives pour les actions inter-modules dans Unit4.

C8 – Suivi et correction des erreurs (intégralité du traitement)

Les systèmes, programmes et travaux essentiels à Unit4 font l'objet d'un suivi, et les erreurs de traitement sont corrigées pour assurer l'intégrité du traitement.

C9 – Logiciels antivirus

Les postes et serveurs de la Ville de Lévis sont protégés par des logiciels antivirus.

C10 – Correctifs de sécurité à jour

Les correctifs de sécurité sont à jour pour les postes de travail, Unit4 et ses bases de données ainsi que les systèmes d'exploitation des serveurs. Les décisions de retarder la mise en place d'un correctif de sécurité sont documentées.


Lévis
VÉRIFICATEUR
GÉNÉRAL

Organismes ayant bénéficié d'une subvention d'au moins 100 000 $

Audit de conformité

CHAPITRE 4

Lévis | VÉRIFICATEUR GÉNÉRAL

Contexte et exigences spécifiées

L'article 107.9 de la *Loi sur les cités et villes* (LCV) énumère les exigences suivantes à l'égard, d'une part, des personnes morales qui bénéficient d'une subvention annuelle et, d'autre part, de l'auditeur externe qui a délivré un rapport d'audit sur leurs états financiers :

> « Toute personne morale qui reçoit une subvention annuelle de la municipalité d'au moins 100 000 $ est tenue de faire vérifier ses états financiers.
>
> Le vérificateur d'une personne morale qui n'est pas visée au paragraphe 2º de l'article 107.7, mais qui reçoit une subvention annuelle de la municipalité d'au moins 100 000 $ doit transmettre au vérificateur général une copie :
>
> 1° des états financiers annuels de cette personne morale;
>
> 2° de son rapport sur ces états;
>
> 3° de tout autre rapport résumant ses constatations et recommandations au conseil d'administration ou aux dirigeants de cette personne morale.
>
> Ce vérificateur doit également, à la demande du vérificateur général :
>
> 1° mettre à la disposition de ce dernier, tout document se rapportant à ses travaux de vérification ainsi que leurs résultats;
>
> 2° fournir tous les renseignements et toutes les explications que le vérificateur général juge nécessaires sur ses travaux de vérification et leurs résultats.
>
> Si le vérificateur général estime que les renseignements, explications, documents obtenus d'un vérificateur en vertu du deuxième alinéa sont insuffisants, il peut effectuer toute vérification additionnelle qu'il juge nécessaire. »

Dans le présent rapport, le terme « organisme » est utilisé pour désigner les personnes morales assujetties à la LCV.

L'audit des états financiers requis par la LCV fournit une reddition de qualité de la part des organismes assujettis. Le regard indépendant et objectif des auditeurs externes est essentiel pour assurer l'intégrité de l'information.

Objectifs de la mission

Nous avons réalisé une mission d'assurance raisonnable de la conformité aux exigences spécifiées à l'article 107.9 de la LCV.

Les objectifs de la mission étaient, d'une part, de s'assurer que les personnes morales ayant obtenu des subventions annuelles de 100 000 $ ou plus au cours de leurs exercices financiers terminés en 2023 ou en 2024 et leur vérificateur externe se sont conformés aux exigences de l'article 107.9 de la LCV et, d'autre part, de déterminer si des travaux de vérification additionnelle étaient nécessaires.

Portée

Aux fins de nos travaux, un organisme est considéré comme assujetti à l'article 107.9 de la LCV lorsqu'une subvention de 100 000 $ ou plus lui est accordée pour chacun de ses exercices financiers terminés au cours des années 2023 et 2024.

Le terme « subvention » n'étant pas précisément défini dans le *Manuel de comptabilité* pour le secteur public de CPA Canada ni dans le *Manuel de présentation de l'information financière municipale* (MPIFM), nous avons utilisé, pour le définir, les critères de paiements de transfert établis dans la norme SP 3410 du *Manuel de comptabilité pour le secteur public* de CPA Canada :

> « Les paiements de transferts sont des transferts d'actifs monétaires ou d'immobilisations corporelles par un gouvernement à un particulier, à une organisation ou à un autre gouvernement, au titre desquels le gouvernement cédant :
>
> - Ne reçoit directement aucun bien ou service en contrepartie, comme dans le cas d'une opération d'achat / de vente ou d'une autre opération d'échange;
> - Ne s'attend pas à être remboursé ultérieurement, comme dans le cas d'un prêt;
> - Ne s'attend pas à obtenir un rendement financier direct, comme dans le cas d'un placement. »

Le MPIFM exige que la plupart des crédits pour taxes soient comptabilisés à titre de subventions. En conséquence, les crédits pour taxes sont inclus dans la portée des subventions, même si aucun transfert d'actifs monétaires ou d'immobilisation n'est en cause.

L'audit de 2024 couvre les personnes morales présentées au tableau suivant, selon la liste établie par la direction des finances et de la trésorerie de la Ville de Lévis.

Tableau 1 : Liste des organismes subventionnés assujettis à l'article 107.9 de la LCV

		Subvention versée au cours de l'exercice (dollars)	
Organismes	**Fin d'exercice**	**2024**	**2023**
Alliance-Jeunesse Chutes-de-la-Chaudière	31 mars	264 905	215 001
Centre aide et prévention jeunesse de Lévis	31 mars	247 079	246 427
Maison de soins palliatifs du Littoral	30 juin	101 300	102 000
Diffusion Avant-Scène	31 décembre	232 819	230 613
Diffusion culturelle de Lévis	31 décembre	580 975	542 902
Patro de Lévis	31 décembre	744 519	703 900
L'Espace culturel du Quartier de Saint-Nicolas	31 décembre	209 058	206 078
Mon Quartier de Lévis	31 décembre	447 263	308 955
Centre socio-culturel et sportif St-Étienne Inc.	31 mai	269 218	268 551

Responsabilité de la direction des finances et de la trésorerie de la Ville de Lévis

La direction des finances et de la trésorerie de la Ville de Lévis est responsable de fournir la liste des organismes auxquels des sommes répondant à la définition de subvention annuelle décrite précédemment à la section « Portée » ont été versées ou octroyées. Elle est aussi responsable de maintenir le système de contrôle interne pour s'assurer que la liste est complète et exacte aux fins de cet audit.

La direction des finances et de la trésorerie de la Ville de Lévis est responsable de transmettre à la vérificatrice générale toutes les informations dont elle a connaissance et qui sont pertinentes eu égard à la mission.

Responsabilités de la direction des organismes subventionnés et de leur auditeur (vérificateur) externe

La direction des organismes subventionnés et de leur vérificateur externe sont responsables de la conformité aux exigences spécifiées.

Responsabilité de la vérificatrice générale de la Ville de Lévis

Notre responsabilité consiste à exprimer une opinion sous forme d'assurance raisonnable sur la conformité des organismes et de leur vérificateur externe aux exigences spécifiées, sur la base des éléments probants obtenus. Nous avons effectué notre mission d'assurance raisonnable conformément aux normes canadiennes de missions de certification (NCMC) - *Missions* d'appréciation directe (NCMC 3001) et *Missions* d'appréciation directe visant la délivrance d'un rapport sur la conformité (NCMC 3531). Ces normes requièrent que nous planifiions et réalisions la mission de façon à obtenir l'assurance raisonnable que les responsables se sont conformés, dans tous les aspects importants, aux exigences spécifiées.

L'assurance raisonnable correspond à un niveau élevé d'assurance, qui ne garantit toutefois pas qu'une mission réalisée conformément aux normes permettra de toujours détecter tout cas important de non-conformité aux exigences spécifiées qui pourrait exister. Les cas de non-conformité peuvent résulter de fraudes ou d'erreurs, et ils sont considérés comme importants 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 sur la conformité implique la mise en œuvre de procédures en vue d'obtenir des éléments probants concernant la conformité aux exigences spécifiées. La nature, le calendrier et l'étendue des procédures choisies relèvent de notre jugement professionnel, et notamment de notre évaluation des risques de non-conformité importante, que celle-ci résulte de fraudes ou d'erreurs.

La mission a porté sur les exercices financiers des organismes se terminant au cours de l'année 2023 et 2024. Nos travaux d'audit ont pris fin le 03 juin 2025.

Travaux effectués

Nos travaux ont consisté à :

- obtenir de la direction des finances et de la trésorerie de la Ville la liste des organismes assujettis à l'article 107.9 de la LCV;
- obtenir la documentation du vérificateur externe de chacun des organismes dont l'exercice financier se termine en 2023 ou en 2024, à savoir :
  - les états financiers annuels ainsi que son rapport sur ces états financiers;
  - tout autre rapport résumant ses constatations et recommandations au conseil d'administration ou aux dirigeants de ces organismes.
- évaluer, à la lumière de cette documentation, si une vérification additionnelle était nécessaire de notre part. À cette fin, nous avons entre autres tenu compte de l'importance des frais d'administration par rapport aux dépenses de livraison de leurs programmes.

Il est important de préciser que nous n'avons effectué aucune vérification des comptes ou documents des organismes concernés quant à l'utilisation appropriée des subventions provenant de la Ville de Lévis.

À la suite de notre évaluation, nous avons contacté la direction de l'organisme Le Patro de Lévis Inc. et son auditeur externe pour discuter de l'allocation des dépenses au titre de dépenses d'administration.

Les éléments probants que nous avons obtenus sont suffisants et appropriés pour fonder notre opinion.

Indépendance et contrôle qualité

Nous nous sommes conformés aux règles et 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.

La vérificatrice générale applique les Normes canadiennes de gestion de la qualité (NCGQ 1 et 2) du Manuel de CPA Canada – Certification. Ainsi, elle conçoit et maintient un système de gestion de la qualité qui comprend des procédures internes documentées en ce qui concerne la conformité aux règles de déontologie, aux normes professionnelles et aux exigences légales et réglementaires applicables, et veille au bon fonctionnement de ce système. Au cours de ses travaux, la vérificatrice générale se conforme aux règles sur l'indépendance et aux autres règles prévues dans son code de déontologie, lesquelles reposent sur les principes fondamentaux d'intégrité, d'objectivité, de compétence professionnelle et de diligence, de confidentialité et de conduite professionnelle.

Opinion

À notre avis, les responsables concernés se sont conformés, dans tous les aspects importants, aux exigences spécifiées à l'article 107.9 de la LCV pour les organismes qui ont obtenu des subventions au cours de leur exercice financier terminé en 2023 ou en 2024. Les états financiers des organismes ont tous fait l'objet d'un audit par un auditeur indépendant, et les rapports résumant leurs constatations et recommandations au conseil d'administration ou aux dirigeants des organismes nous ont été remis.

À la suite de l'examen de ces documents, à l'exception des états financiers de l'organisme le Patro de Lévis, aucune vérification additionnelle n'a été jugée nécessaire.

Pour le Patro de Lévis, les états financiers audités présentaient des dépenses d'administration dépassant légèrement 60 % du total des dépenses de l'organisme pour les exercices financiers clos en décembre 2022 et 2023. Estimant cette proportion déraisonnable pour un organisme subventionné, la vérificatrice générale a discuté avec la direction du Patro de Lévis des bases utilisées pour allouer ces dépenses et formulé des recommandations. La direction du Patro de Lévis et l'auditeur externe ont démontré que la base d'allocation devait être modifiée pour bien refléter les activités de l'organisme. L'information a été redressée dans les états financiers audités de l'exercice se terminant le 31 décembre 2024. Les principales catégories de dépenses qui ont été exclues des dépenses d'administration sont les suivantes :

- les salaires et charges sociales de sept employés, selon la proportion de leur temps consacré aux opérations;
- les frais généraux attribuables aux opérations et les frais d'occupation des locaux attribués aux opérations.

À la suite de cette correction, la proportion des dépenses d'administration s'élève à 25,7 % du total des dépenses du Patro de Lévis pour l'exercice financier clos en décembre 2023 (13,2 % en 2024).

Nous ne fournissons aucun avis juridique relativement à la conformité des responsables concernés aux exigences spécifiées.

Commentaires de la direction générale

La direction générale de la Ville de Lévis partage l'opinion de la vérificatrice générale sur le fait que les frais d'administration présentés aux états financiers audités du Patro de Lévis ne sont pas raisonnables. Nous avons accompagné la direction du Patro de Lévis dans son plan d'action pour corriger l'erreur de présentation de cette information financière. Même si la préparation des états financiers des organismes assujettis à l'article 107.9 de la LCV est de la responsabilité exclusive de la direction des organismes, à compter de janvier 2025, un expert de la direction des finances et trésorerie, qualifié en tant que CPA auditeur, examinera les états financiers audités des organismes assujettis pour les aider à respecter leurs obligations de reddition de comptes envers la vérificatrice générale.

Précisons que la direction de la Ville de Lévis qui a octroyé la subvention effectue un suivi auprès des organismes pour s'assurer qu'ils contribuent à la qualité de vie de la communauté lévisienne selon les conditions qu'ils se sont engagés à respecter dans l'entente de subvention. Le rapport annuel du Patro de Lévis fait état de cette contribution sociale obtenue grâce aux 14950 heures de services gratuits fournis par ses bénévoles en 2024 (10 818 heures en 2023).


Lévis
VÉRIFICATEUR GÉNÉRAL

Suivi de l’implantation des recommandations formulées lors d’audits antérieurs

CHAPITRE 5

Lévis | VÉRIFICATEUR GÉNÉRAL

Suivi des recommandations

L'objectif du suivi des recommandations est d'assurer que celles-ci ont été appliquées dans un délai raisonnable, et que les mesures prises ont permis de corriger les lacunes observées.

Lorsqu'une mission d'audit est achevée, les deux dernières étapes que la Ville doit effectuer sont de :

1. préparer un plan d'action détaillé;
2. mettre en œuvre ce plan d'action.

Préparation d'un plan d'action détaillé

La direction auditée est invitée à produire un plan d'action pour atteindre les objectifs de chacune des recommandations et agir sur les causes des lacunes soulevées dans le rapport d'audit. Le plan d'action doit présenter les solutions de mitigation choisies, le nom des personnes responsables de leur mise en place ainsi que la date cible pour achever les travaux. Bien que seule la direction du service audité soit responsable de son élaboration, la vérificatrice générale (VG) analyse et approuve le plan d'action.

La direction de la Ville a répondu avec diligence pour préparer le plan d'action des recommandations émises à la suite de l'audit des CGI. Quant aux recommandations sur la Gestion des risques liés à la PRP dont l'audit s'est terminé le 2 juillet 2025, la vérificatrice générale a demandé à la direction de présenter son plan d'action détaillé avant la fin de l'année 2025.

Tableau I : Statut sur la préparation des plans d'action

Mandat d'audit	Rédaction du plan d'action	Date cible pour la mise en place
Contrôles généraux informatiques	Achevé et approuvé par la VG	Juin 2026
Gestion des risques liés à la protection des renseignements personnels	Non commencé (recommandations soumises à la direction générale le 2 juillet 2025)	À définir

Mise en œuvre des plans d'action

La direction auditée est responsable de la mise en œuvre des plans d'action dans des délais raisonnables et du fonctionnement efficace des mesures de mitigation qu'ils énoncent. Lorsque des plans d'action sont mis en œuvre sur une période de plus d'un an, elle doit s'assurer de prendre en compte l'évolution du contexte pour que les solutions choisies demeurent appropriées au moment de leur implantation. Elle doit discuter avec la VG des modifications à apporter aux plans d'action, le cas échéant.

La VG effectue un suivi de la mise en œuvre des plans d'action en recueillant les déclarations des gestionnaires et en examinant certains documents pertinents, afin d'évaluer si des mesures suffisantes ont été prises en réponse aux recommandations. Son équipe évalue aussi le degré d'avancement de l'implantation de ces mesures, selon les dates cibles établies aux plans d'action. Soulignons que cet examen ne vise pas à certifier la mise en œuvre des mesures liées aux recommandations, et qu'aucun rapport d'audit n'est produit sur le suivi des recommandations.

Le dernier rapport publié du vérificateur général de la Ville de Lévis remonte à l'année 2021. Le suivi des recommandations a été effectué pour les recommandations émises entre 2015 et 2021 (voir le tableau II).

Tableau II : Statut d'avancement de la mise en œuvre des plans d'action

Mandat d'audit par entité juridique	année	Recommandations				Appréciation de la vérificatrice générale
		Émises	Appliquées	Application en cours	Application non débutée	
Ville de Lévis						
Octroi des contrats de 100 000 dollars et plus	2015	14	14			satisfaisant
Gestion des stocks de biens non durables	2016	10	9	1		satisfaisant
Gestion des grands projets	2016	8	7	1		satisfaisant
Acquisitions de services professionnels et de services techniques	2017	8	8			satisfaisant
Acquisitions d'immeubles	2018	8	8			satisfaisant
Gestion de l'entretien correctif des bâtiments	2019	4		4		partiellement satisfaisant
Gestion des actifs	2019	6	1	5		partiellement satisfaisant
Gestion de l'entretien du matériel roulant	2019	11	11			satisfaisant
Gestion financière	2021	9	9			satisfaisant
Total		**78**	**67**	**11**	**0**	
Société de transport de la Ville de Lévis						
Entretien des véhicules	2020	21	21			satisfaisant
Total		**21**	**21**	**0**	**0**	
Office municipal d'habitation de Lévis						
Entretien des immeubles	2017	15	15			satisfaisant
Processus de remplacement des locataires	2020	8	8			satisfaisant
Total		**23**	**23**	**0**	**0**	

Commentaires sur la mise en œuvre des recommandations

Gestion des stocks de biens non durables (2016)

L'information reçu de la Direction de la gestion du capital humain et de la Direction de l'approvisionnement et de la gestion immobilière est à l'effet que les mesures mises en œuvre ont permis de corriger les lacunes de 9 des 10 recommandations énoncées dans ce rapport de 2016. Voici la recommandation qui n'est pas encore appliquée :

> **V16-17** Procéder au suivi des recommandations de la firme externe découlant de l'audit des équipements pétroliers et faire la mise à jour de l'inventaire des réservoirs pétroliers.

La Ville de Lévis a mandaté une firme spécialisée en 2022, puis de nouveau en 2024-2025, afin d'inspecter l'ensemble des équipements pétroliers, de mettre à jour l'inventaire et de formuler des recommandations couvrant tous les réservoirs municipaux. Une estimation budgétaire ventilée par réservoir a également été produite pour planifier les interventions. Une rencontre est prévue en juillet 2025 en vue de clarifier les rôles et responsabilités des intervenants et intervenantes. Les analyses sont toujours en cours, et les plans d'action restent à finaliser.

Gestion des grands projets (rapport de 2016)

Selon l'information fournie par la Direction du génie et la Direction de l'approvisionnement et de la gestion immobilière, les mesures mises en œuvre ont permis de corriger les lacunes de 7 des 8 recommandations de ce rapport. La recommandation V16-3 sur la gouvernance des projets d'envergure ou atypiques est en cours d'application.

Gestion de l'entretien correctif des bâtiments (rapport de 2019)

La Direction de l'entretien des infrastructures a beaucoup approfondi ses réflexions, notamment pour la recommandation V19-9 sur l'usage des technologies de l'information. Elle a ainsi mieux défini ses besoins et sera en mesure de bénéficier de l'évolution des technologies disponibles, notamment en intelligence artificielle. Elle travaille présentement à redéfinir les processus cibles pour saisir cette opportunité.

La mise en œuvre du plan d'action initial lié à ce rapport est en retard. Un nouveau plan d'action est en préparation et sera analysé par la VG à l'automne 2025. Le niveau d'avancement se situe entre 30% et 90%, selon les recommandations.

Gestion des actifs (rapport de 2019)

Lorsque ce rapport d'audit a été rédigé, en 2019, le ministère des Affaires municipales et de l'Habitation (MAMH) n'avait pas précisé ses attentes concernant la gestion des actifs des municipalités. Lors de la mise en place du programme de subventions PRIMEAU, destiné aux investissements dans les infrastructures en eau des municipalités, le MAMH a priorisé la gestion des actifs en eau et proposé une feuille de route sur les mesures à prendre. Pour respecter ces exigences et s'assurer d'obtenir les subventions disponibles, la Direction du génie déploie ses actions selon la feuille de route du MAMH et la vérificatrice générale effectue le suivi des recommandations sur cette même base, à laquelle elle a ajouté la gestion du réseau routier ainsi que des trottoirs et pistes cyclables.

Les lacunes de la recommandation concernant la définition des besoins d'expertise et la formation du personnel (V19-6) ont été corrigées. L'avancement des travaux, évalué comme partiellement satisfaisant, s'est accéléré dans les derniers mois. L'orientation no1du plan stratégique 2025-2030 précise que la conception et le déploiement du plan de gestion d'actifs en eau est une priorité de la Ville.

Gestion financière (rapport de 2021)

La mise en œuvre du plan d'action lié au rapport sur la gestion financière est terminée. La plus grande avancée réside dans l'application des recommandations sur la planification financière à long terme, notamment la préparation et l'approbation du cadre financier et des politiques financières qui lui sont associées (politique de gestion de la dette et politique de gestion des excédents et des réserves). Notons aussi que la DG a démontré, en présentant son budget 2025, que le cadre financier adopté par le conseil municipal en 2025 a été respecté.

En ce qui concerne la recommandation V21-05 c) *S'assurer d'utiliser des ratios financiers pertinents et d'en faire une bonne interprétation, en privilégiant la prise en compte de sa situation financière sur un horizon raisonnable*, nous avons remarqué une meilleure utilisation de ratios comparables. La VG a mentionné à la direction générale la nécessité d'être vigilant concernant la comparaison des taux de taxation. En effet, les taux de taxation des villes de Lévis, de Québec, de Sherbrooke, de Saguenay, de Terrebonne et de Trois-Rivières ne sont pas vraiment comparables puisque seules Lévis et Terrebonne ont la même date d'évaluation foncière. L'impact des dates du rôle triennal est particulièrement important dans le marché immobilier en hausse forte et constante des dernières années.


Lévis
VÉRIFICATEUR
GÉNÉRAL

Relevé des dépenses d'opération
du bureau de la vérificatrice générale

ANNEXE

Lévis | VÉRIFICATEUR GÉNÉRAL

Bureau de la vérificatrice générale de la Ville de Lévis

Relevé des dépenses d'opérations
Pour l'exercice terminé le 31 décembre 2024

Accompagné du rapport de l'auditeur indépendant

MALLETTE

Mallette S.E.N.C.R.L.
200-3075 chemin des Quatre-Bourgeois
Québec QC G1W 5C4

Téléphone : 418 653-4431
Télécopie : 418 656-0800
info.quebec@mallette.ca

RAPPORT DE L'AUDITEUR INDÉPENDANT

Aux membres du conseil municipal,

Opinion

Nous avons effectué l'audit du relevé des dépenses d'opérations (informations financières) du Bureau de la vérificatrice générale de la Ville de Lévis pour l'exercice terminé le 31 décembre 2024, ainsi que la note complémentaire, y compris le résumé des principales méthodes comptables.

À notre avis, les informations financières ci-jointes ont été préparées, dans tous leurs aspects significatifs, conformément aux méthodes comptables décrites à la note 1.

Fondement de l'opinion

Nous avons effectué notre audit conformément aux normes d'audit généralement reconnues du Canada. Les responsabilités qui nous incombent en vertu de ces normes sont plus amplement décrites dans la section « Responsabilités de l'auditeur à l'égard de l'audit des informations financières » du présent rapport. Nous sommes indépendants du Bureau de la vérificatrice générale de la Ville de Lévis conformément aux règles de déontologie qui s'appliquent à l'audit des informations financières au Canada et nous nous sommes acquittés des autres responsabilités déontologiques qui nous incombent selon ces règles. Nous estimons que les éléments probants que nous avons obtenus sont suffisants et appropriés pour fonder notre opinion d'audit.

Autre point - Restriction à l'utilisation

Les informations financières ont été préparées afin de satisfaire aux exigences de l'article 108.2.1 de la Loi sur les cités et villes (L.R.Q., chapitre C-19). En conséquence, il est possible que les informations financières ne puissent se prêter à un usage autre.

Responsabilités de la direction et des responsables de la gouvernance à l'égard des informations financières

La direction du Bureau de la vérificatrice générale de la Ville de Lévis est responsable de la préparation des informations financières conformément aux méthodes comptables décrites à la note 1 ainsi que du contrôle interne qu'elle considère comme nécessaire pour permettre la préparation d'informations financières exemptes d'anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs.

Il incombe aux responsables de la gouvernance de surveiller le processus d'information financière du Bureau de la vérificatrice générale de la Ville de Lévis.

Responsabilités de l'auditeur à l'égard de l'audit des informations financières

Nos objectifs sont d'obtenir l'assurance raisonnable que les informations financières prises dans leur ensemble sont exemptes d'anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs, et de délivrer un rapport de l'auditeur contenant notre opinion. L'assurance raisonnable correspond à un niveau élevé d'assurance, qui ne garantit toutefois pas qu'un audit réalisé conformément aux normes d'audit généralement reconnues du Canada permettra toujours de détecter toute anomalie significative qui pourrait exister. Les anomalies peuvent résulter de fraudes ou d'erreurs et elles sont considérées comme significatives lorsqu'il est raisonnable de s'attendre à ce que, individuellement ou collectivement, elles puissent influer sur les décisions économiques que les utilisateurs des informations financières prennent en se fondant sur celles-ci.

Dans le cadre d'un audit réalisé conformément aux normes d'audit généralement reconnues du Canada, nous exerçons notre jugement professionnel et faisons preuve d'esprit critique tout au long de cet audit. En outre :

- Nous identifions et évaluons les risques que les informations financières comportent des anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs, concevons et mettons en œuvre des procédures d'audit en réponse à ces risques, et réunissons des éléments probants suffisants et appropriés pour fonder notre opinion. Le risque de non-détection d'une anomalie significative résultant d'une fraude est plus élevé que celui d'une anomalie significative résultant d'une erreur, car la fraude peut impliquer la collusion, la falsification, les omissions volontaires, les fausses déclarations ou le contournement du contrôle interne;
- Nous acquérons une compréhension des éléments du contrôle interne pertinents pour l'audit afin de concevoir des procédures d'audit appropriées aux circonstances, et non dans le but d'exprimer une opinion sur l'efficacité du contrôle interne de la Ville de Lévis;
- Nous apprécions le caractère approprié des méthodes comptables retenues et le caractère raisonnable des estimations comptables faites par la direction, le cas échéant, de même que des informations y afférentes fournies par cette dernière.

Nous communiquons aux responsables de la gouvernance notamment l'étendue et le calendrier prévus des travaux d'audit et nos constatations importantes, y compris toute déficience importante du contrôle interne que nous aurions relevée au cours de notre audit.

Mallette S.E.N.C.R.L. [1]
Mallette S.E.N.C.R.L.
Société de comptables professionnels agréés

Québec, Canada
Le 25 avril 2025

[1] CPA auditrice, permis de comptabilité publique nº A125052

BUREAU DE LA VÉRIFICATRICE GÉNÉRALE DE LA VILLE DE LÉVIS

Relevé des dépenses d'opérations (en dollars)
Pour l'exercice terminé le 31 décembre 2024

	Budget	Dépenses	
		2024	2023
Ressources humaines :			
Internes	385 934 $	389 919 $	168 268 $
Externes	630 852	94 220	164 110
	1 016 786	484 139	322 378
Dépenses d'opérations	8 500	7 966	13 457
Total :	**1 025 286 $**	**492 105 $**	**345 835 $**

Note complémentaire

Note 1. Principales méthodes comptables

Le relevé des dépenses d'opérations du Bureau de la vérificatrice générale de la Ville de Lévis est préparé et établi conformément aux normes comptables pour le secteur public au Canada. Il répond également aux exigences de l'article 108.2.1 de la Loi sur les cités et villes (LCV) du Québec.

La comptabilisation des transactions s'effectue selon la méthode de la comptabilité d'exercice.

Les dépenses d'opérations ne comprennent que celles qui ont été directement engagées par la vérificatrice générale de la Ville de Lévis.

Le budget inclut les crédits budgétaires de 451 922 $ accordés au Bureau de la vérificatrice générale de la Ville de Lévis qui n'avaient pas encore été utilisés au 1er janvier 2024. Les crédits budgétaires accordés à la vérificatrice générale selon l'article 107.5 de la LCV sont octroyés de façon permanente. Le report des crédits budgétaires non utilisés a été confirmé par la résolution du conseil de la Ville de Lévis tenue le 26 juin 2018 (CV-2018-04-59). Ces crédits proviennent de l'excédent de fonctionnement non affecté.

Déclaration — Je déclare que les informations contenues dans ce rapport correspondent à la situation telle qu'elle se présentait le 24 février 2025.

La vérificatrice générale,

(Original signé par la vérificatrice générale)

Francine Tessier, CPA auditrice

Lévis | VÉRIFICATEUR GÉNÉRAL

Lévis | VÉRIFICATEUR GÉNÉRAL

ville.levis.qc.ca