INTERNAL AUDIT REPORT

Office of the City Solicitor

Program Review: Privacy Management

Assignment # 24-03

INTERNAL AUDIT REPORT

Office of the City Solicitor

Program Review: Privacy Management

Assignment # 24-03

Sean McGrath, CPA,
CA, CIA, CFE
Senior Internal Auditor
Date: April 7, 2025

Sean P. Janes, CPA,
CMA, CIA, CFE
City Internal Auditor
Date: April 7, 2025

TABLE OF CONTENTS

To: Chair & Committee Members, City of St. John's Audit Committee

Area Responsible: Cheryl Mullett, City Solicitor

Copy to: Kevin Breen, City Manager

INTRODUCTION

OBJECTIVE

In accordance with the City of St. John's ("City") 2024 approved audit plan (SJMC-R-2024-04-30/197), the objectives of the audit were to:

- Determine if the City of St. John's is in compliance with various aspects of the provincial Access to Information and Protection of Privacy Act, 2015 and related internal City policy and procedure.

- Identify opportunities to improve the effectiveness and efficiency of supporting processes, if applicable.

BACKGROUND

Access to Information and Protection of Privacy

The Access to Information and Protection of Privacy Act, 2015 ("Act") is provincial legislation that is designed to create a culture of openness and accountability in the public sector while protecting personal information and other types of sensitive information[1]. It applies to all public bodies in Newfoundland and Labrador, including municipalities. The Act is broken down into five separate parts, with the majority of the provisions either relating to the access and correction of information (Part II) or the protection of personal information (Part IV).

[1]Newfoundland and Labrador Access to Information and Protection of Privacy Office. *Welcome to the Access to Information and Protection of Privacy Office.* https://www.gov.nl.ca/atipp/

Section 3 of the Act outlines its purpose, which is to facilitate democracy through:

- ensuring citizens have the information required to participate meaningfully in the democratic process.

- increasing transparency and accountability of public bodies, elected officials, and employees of Public Bodies.

- protecting the privacy of individuals with respect to the personal information that public bodies hold about them.

As noted on the City of St. John's website, the City recognizes the public's right to access records as a vital part of maintaining an accountable and transparent government. The City is also committed to protecting personal information as it may only be collected, used, accessed, and disclosed in accordance with the Act.

Access to Information and Protection of Privacy Function

An Access to Information and Protection of Privacy ("ATIPP") function is in place at the City to help implement the Act and City Policy 01-04-02, Privacy Management Policy. The policy, along with its related procedures, provides a framework for a variety of privacy-related activities throughout the organization, such as establishing controls for personal information, protecting the personal information in the custody and/or control of the City, and protecting the privacy of individuals.

The City's ATIPP function consists of two access and privacy analysts ("ATIPP Analysts"). Prior to 2024, this function was overseen by the Office of the City Clerk, with the City Clerk serving as the designated head of the public body ("Head") for the City. According to the Act, the Head is legislatively responsible for all actions and decisions made by the public body.

In September 2024, the reporting structure changed, resulting in the ATIPP function now reporting to the Office of the City Solicitor, which is part of the Office of the City Manager. As a result of this reorganization, the City Manager has taken over the role as Head under the Act, replacing the City Clerk. This change was formally approved by the City of St. John's Council ("Council") on September 3, 2024.

Roles and Responsibilities

As required by the Act, the Head shall designate a person on the staff of a public body as the Coordinator. Although the Head is ultimately responsible for the actions of the public body, it is the role of the Coordinator that facilitates the day-to-day activities of the ATIPP function.

Both ATIPP Analysts share in the role of the Coordinator at the City of St. John's. The Coordinator has legislated responsibilities under the Act, including receiving and processing access to information requests, coordinating responses to requests for approval by the Head, and educating staff of the public body about applicable provisions of the Act. Other duties involve developing and managing privacy policy, procedures, guidelines, and templates, providing support to City staff, investigating privacy breaches, and consulting with the Government of Newfoundland and Labrador's ATIPP Office and the Office of the Privacy Commissioner as needed.

Under the current reporting structure, the City Solicitor manages the ATIPP Analysts and is administratively responsible for the ATIPP function. However, given the nature of their work and their legislated responsibilities, the ATIPP Analysts operate with a large degree of autonomy.

While the ATIPP Analysts are tasked with specific duties relating to access and privacy, all employees have a role to play in privacy management at the City. At a minimum, all employees must comply with City Policy 01-04-02, Privacy

Management Policy, and related procedures, and be vigilant when changing, collecting, using, or disclosing personal information.

Personal Information

Personal information, as defined in the Act, means recorded information about an identifiable individual. A variety of details can constitute personal information, including an individual's name, address, telephone number, race, religious beliefs, age, sex, marital status, etc. Personal information can also include an identifying number, symbol, or other identifier assigned to the individual, as well as information regarding inheritable characteristics such as fingerprint and blood type information. Details relating to a person's medical, educational, financial, criminal, and employment history are also considered personal information under the Act. As outlined in City Policy 01-04-02, Privacy Management Policy, the term 'personal information' has the same meaning at the City as it does under the Act.

The Act, as well as City policy and procedure, outlines numerous privacy mechanisms and tools that help public bodies protect personal information that is under their custody and/or control. Such mechanisms include, but are not limited to, privacy impact assessments, personal information banks and inventories, and records safeguard plans.

Preliminary Privacy Impact Assessments and Privacy Impact Assessments

The City's Privacy Assessment Procedures define a preliminary privacy impact assessment ("PPIA") as a preliminary assessment to identify the privacy implications of a City project and to determine whether a privacy impact assessment ("PIA") should be completed for the project. A privacy impact assessment is defined as an assessment to determine if a current or proposed project meets or will meet the requirements of the Access to Information and Protection of Privacy Act.

The City's Privacy Assessment Procedures require program managers to complete a PPIA for any new or substantially modified project that accesses, collects, uses, discloses, or disposes of personal information. Once completed, the PPIA must be sent to an ATIPP Analyst prior to advancing any direction or decision notes for approval. If no direction or decision note is required, the PPIA shall be completed and forwarded to an ATIPP Analyst prior to the implementation of the program or project. The results of the PPIA determines if a more comprehensive review of privacy issues is required through the completion of a full PIA.

Section 72 of the Act also details PPIA and PIA requirements. However, these provisions are only a legislative requirement for departments and branches of the executive government of Newfoundland and Labrador. Therefore, PPIA and PIA requirements are a policy requirement for the City of St. John's rather than a legislative obligation.

However, during the last statutory review of the Act, the Access to Information and Protection of Privacy Act Statutory Review 2020 Committee[2] ("ATIPPA Review Committee") recommended that the section 72 provision be extended to specifically include the City of St. John's as well as other larger municipalities. Although the Act was not subsequently amended to extend the application of section 72, it is scheduled to undergo a statutory review again in 2025.

Personal Information Banks and Personal Information Inventory

City Policy 01-04-02, Privacy Management Policy, defines a personal information bank ("PIB") as personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol, or other particular assigned

[2] The Access to Information and Protection of Privacy Act, 2015, mandates that an independent review committee, appointed by the NL Minister of Justice and Public Safety, conduct a comprehensive review of the Act's provisions and operations at least every five years. The most recent review took place in 2020, chaired by the Honourable David B. Orsborn. The full report can be found at https://www.nlatippareview.ca/files/FINAL-REPORT-June-8-2021-2.pdf

to an individual. The policy also defines a personal information inventory ("PII") as an inventory of all the City's PIBs.

PIBs and PIIs are further detailed in the City's Personal Information Bank and Inventory Procedures. The procedure requires each division at the City to identify the collections of personal information it has in its custody and submit the PIB listings to an ATIPP Analyst. Following receipt of all departmental PIB listings, an ATIPP Analyst is responsible for developing a single PII for publication on the City's website.

Section 111 of the Act, Publication Scheme, also details PIB and PII requirements. It notes that the Head is responsible for publishing information, including PIBs, to assist in identifying and locating records in the custody and/or control of public bodies. However, section 111 is only applicable to those public bodies listed in the ATIPP Regulations. As no public bodies are listed in the Regulations, the provisions of section 111 are not a legislative requirement for any public body in Newfoundland and Labrador, including the City of St. John's.

However, the ATIPPA Review Committee[2] recommended in 2020 that all public bodies, except small municipalities, be required to create publication schemes. While the Act was not amended to include this recommendation, it may be reconsidered during the next statutory review scheduled for 2025.

Protection of Personal Information and Records Safeguard Plans

City Policy 01-04-02, Privacy Management Policy, requires department heads to ensure appropriate safeguards are in place to protect personal information. These safeguards are further outlined in the City's Personal Information and Record Protection Procedures. This procedural document outlines the requirement for department heads to create records safeguard plans, which document the administrative, technical, access control, and physical safeguards implemented for departmental records containing personal information.

Additionally, the plans should include a description of any deficiencies in the current safeguards and propose steps to address and mitigate these issues.

Although the concept of records safeguard plans is not explicitly mentioned in the Act, section 64 covers the protection of personal information. The section requires the Head to take reasonable steps to ensure that personal information in the custody and/or control of the public body is protected from theft, loss, and other types of unauthorized access or modification. Furthermore, the section stipulates that records must be retained, transferred, and disposed of in a secure manner.

The provisions of section 64 apply to all public bodies and therefore the City of St. John's has a legislative requirement to ensure its records are protected pursuant to the Act.

METHODOLOGY & SCOPE

The scope of the audit included a review of various City ATIPP processes to determine if they are in compliance with the provincial Access to Information and Protection of Privacy Act and/or internal City policy and procedure. The reviewed processes included preliminary privacy impact assessments, privacy impact assessments, personal information banks, personal information inventories, records safeguard plans, and related controls that protect personal information that is under the purview of the City. Unless otherwise noted, all other areas of the Act and corresponding City policy and procedure, such as access to information requests and privacy complaints, were outside the scope of the audit.
In addition to reviewing compliance with the Act and internal policy and procedure, the applicable processes were also reviewed to identify potential opportunities to improve their effectiveness and efficiency. This was achieved by ensuring that processes adhered to guidance recommended by authorities such

as the Office of the Information and Privacy Commissioner of Newfoundland and Labrador.

The audit also examined whether adequate governance processes are implemented and operating effectively to manage and monitor ATIPP activities toward the achievement of its functional objectives. However, the audit did not include any work relating to reviewing the recently revised reporting structure for the ATIPP function, as City management had already conducted a review prior to implementing the change.

Audit procedures were mainly conducted between October 2024 and March 2025 and predominately included discussions with management and an inspection of supporting documentation. Sampling techniques were used when evaluating legislative and/or policy compliance for certain processes (e.g., the privacy impact assessment process). The audit procedures obtained sufficient appropriate audit evidence to meet the audit objectives.

CONCLUSION

The ATIPP function has a variety of effective and efficient processes in place to help the City fulfil its privacy-related obligations under the provincial Access to Information and Protection of Privacy Act and meet its internal policy requirements. These include the implementation of a robust privacy policy (City Policy 01-04-02, Privacy Management Policy), which is supported by detailed procedures, guidance documents, and standardized templates and practices. The City also employs dedicated privacy professionals and ensures that privacy roles and responsibilities are clearly defined, documented, and fully formalized. Additionally, the City has implemented mandatory privacy training for all staff and undertakes awareness activities, such as postings on the City intranet, to further help ensure all employees are aware of their privacy obligations.

However, certain privacy processes at the City can be improved to ensure compliance with internal City policy and procedure. Foremost, the City has an opportunity to enhance the completeness of PPIAs and PIAs by effectively incorporating them into the forthcoming project review process. Steps can also be taken to collect all applicable PIBs and finalize a PII for publication on the City's website. Similarly, ATIPP management should meet with management from the Archives and Records Management Division to determine which division should take ownership of the records safeguard plan requirement and ensure the process is completed.

These recommended improvements, along with the other recommendations noted in the audit report, will help the City of St. John's fulfil its privacy obligations, both under the Act and as required by internal City policy and procedure.

EXECUTIVE SUMMARY

The Office of the City Internal Auditor's ("OCIA") review of Privacy Management focused on whether there are efficient and effective processes in place to help ensure the City of St. John's ("City") fulfils its privacy-related obligations under the provincial Access to Information and Protection of Privacy Act, 2015 ("Act") and meets its internal policy requirements.

Audit testing and procedures utilized during the review identified several positive outcomes. Foremost, there is a significant amount of internal policy and procedure implemented outlining important privacy-related processes at the City. This includes policies and procedures relating to privacy management, privacy assessments, personal information banks and inventories, personal information and records protection, training requirements, etc. Moreover, a number of key processes, such as privacy assessments, are further supported with standardized templates and guidance documents to help ensure they are carried out accurately and completely.

Additionally, City Policy 01-04-02, Privacy Management Policy, requires all employees to complete an Access to Information and Protection of Privacy ("ATIPP") training course. This course informs employees of their legislated responsibilities and provides them with resources and tools to protect personal information that is under the control and/or custody of the City.

Discussions with ATIPP management also indicated that both Access and Privacy Analysts ("ATIPP Analysts") are knowledgeable regarding the provisions of the Act, associated policies and procedures, and various best practices relating to protecting personal information. Both ATIPP Analysts have completed the Information Access and Protection of Privacy Certificate as of March 2025. This achievement further highlights their understanding of access and privacy management.

The audit also noted that efforts have been made to collect Personal Information Banks ("PIBs") from various City divisions. While several PIBs still need to be gathered and a comprehensive personal information inventory must be compiled, the ATIPP function successfully collected over forty PIBs during a project initiated in 2020. Discussions with ATIPP management indicated that they now have the resources to complete this project due to the addition of a second ATIPP Analyst since the project's initial undertaking.

Moreover, at the time of the audit, a project management review process was under development at the City. Although the process had yet to be implemented when the audit fieldwork concluded, the completed process should help mitigate various risks, including privacy risks, that are relevant to most projects. The City should be commended for proactively taking steps to implement such a process.

Nevertheless, the audit identified opportunities for management to improve its internal processes in a number of areas. Foremost, audit testing indicated there are completeness issues regarding privacy impact assessments. As such, steps should be taken to ensure a project management review process is finalized and implemented, and that the process incorporates mechanisms to enhance the completeness of privacy assessments and mitigate project privacy risks. The ATIPP Analysts should have input when determining whether the project management review process is designed to adequately mitigate such risks.

Moreover, the City should consider adopting the Government of Newfoundland and Labrador's privacy assessment process as outlined in the Act. This would likely increase the completeness of preliminary privacy impact assessments, as it would require all projects to formally assess and document whether a project involves personal information.

Furthermore, it is recommended that management identify active projects implemented before 2019 and work with applicable project owners to complete

privacy assessments for those projects. Such projects were implemented prior to the commencement of the privacy assessment process at the City and therefore have never been assessed for privacy risks. Such assessments should be completed as time and resources allow.

Other improvements can be made to the privacy assessment process including potentially developing detective controls to further enhance privacy assessment compliance, undertaking an internal awareness campaign to promote the importance and benefits of completing privacy impact assessments, and updating select project management guidance at the City to include reference to privacy assessments.

Management should also consider implementing algorithmic impact assessments as part of its privacy management program at the City. These assessments are a best practice risk assessment tool designed to help assess and mitigate the impacts associated with deploying an automated decision system.

The audit report also recommends collecting the remaining personal information banks from applicable divisions and posting a full personal information inventory on the City's website. Similarly, management should meet with the Archives and Records Management Division to determine who will take ownership of the records safeguard plan process and ensure the project is completed.

Lastly, management has an opportunity to enhance certain governance processes. Suggested improvements include updating relevant policies, procedures, and forms. Additionally, the City Manager, as the head of the public body, should draft a formal mandate letter to the ATIPP Analysts, who act as the City's ATIPP Coordinator. This letter would outline the City's commitment to fulfilling the objectives of the Act and clarify the roles and responsibilities of all parties involved.

These recommendations, and other observations outlined in the report, will assist the City in its continued efforts to protect personal information and meet its applicable privacy requirements under the Act.

DETAILED ANALYSIS

Section 1 – Privacy Impact Assessments

As outlined in City Policy 01-04-02, Privacy Management Policy, no new or substantially modified project involving the collection, use, or disclosure of personal information shall commence until a preliminary privacy impact assessment ("PPIA") has been completed by the project manager and approved in accordance with the Privacy Assessment Procedures. Depending on the risks identified in the PPIA, further analysis may be required through the completion of a full privacy impact assessment ("PIA"). However, as noted in the City's ATIPP guidelines, it may be obvious at the outset of certain projects that a PIA will be required. In those circumstances, the ATIPP Coordinator ("ATIPP Analyst") will advise the project manager if it is appropriate to forego a PPIA and proceed directly to a PIA.

To determine the extent of PPIA and PIA compliance at the City, the OCIA selected 10[3] projects that collected, used, disclosed, accessed, or disposed of personal information. Given that all the selected projects involved personal information, the OCIA expected to see a completed PPIA or PIA for each project. Testing indicated that 7 of the projects did not have a PPIA or PIA in place.

The testing results were subsequently discussed with the ATIPP Analysts. Through these collaborative discussions, several potential underlying causes were identified to explain why a program manager may fail to complete a required PPIA or PIA. These causes, along with recommended improvements, are discussed in detail in this section (i.e., Section 1) of the report.

[3] At the time of the audit, the City of St. John's did not have a project database or tracking system, making it difficult to establish a reliable sampling population. The OCIA selected project testing samples from council progress reports and other means; however, this was a tedious process as the OCIA had to be reasonably certain that the sampled project contained personal information. This limitation reduced the size of the testing sample.

Issue 1.1 – Project Review Process

A project review process is a centralized, organization-wide approach used to evaluate projects for various risks prior to the project being implemented. This process ensures that a project is not undertaken without the completion of a thorough risk assessment and that actions are taken to mitigate identified risks. Moreover, the process helps deter a silo mentality for project managers. Such a mentality is detrimental to an organization, as it leads to project teams operating in isolation, thus hindering information sharing across the organization.

From a privacy perspective, the importance of a project review process is highlighted by the Office of the Privacy Commissioner of Canada. The office notes that inadequate project screening is the most common control weakness relating to PPIA and PIA compliance and that the absence of a screening process effectively contributes to instances of PIA omission.[4, 5]

Discussions with management at various points in 2024 indicated that while the City did not have a formal project review process in place at the time, it was in the preliminary stages of developing a similar mechanism. Under the proposed process, departmental staff would first be required to obtain project approval from the City's Senior Executive Committee ("SEC"), which is comprised of senior City staff, prior to initiating their projects.

If a project receives SEC approval, it would then be forwarded to the Organizational Performance and Strategy team for project support. As part of this process, the project lead would be responsible for completing a standardized assessment form to evaluate key implications of the project. This form would address areas such as budget, procurement, legal compliance, communications,

[4] Office of the Privacy Commissioner of Canada. (2007). *Assessing the Privacy Impacts of Programs, Plans, and Policies.* https://www.priv.gc.ca/en/opc-actions-and-decisions/audits/pia_200710/
[5] Office of the Privacy Commissioner of Canada. (2025). OPC's Guide to the Privacy Impact Assessment Process. https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/

information services, policy alignment, human resources, and privacy considerations.

Although this process was not in place by the conclusion of the audit fieldwork in early 2025, management was hopeful that it, or a similar approach, would be implemented sometime during the year. Depending on how the project review process is designed and implemented, it could significantly improve PPIA and PIA compliance.

Recommendation 1.1

To help mitigate privacy risks, the City of St. John's should:

i. Implement a formal project review process. The process should include a mechanism to ensure that reviewed projects are appropriately evaluated for privacy risks.

ii. Develop and implement policies and/or procedures outlining the project review process.

Priority Level: P1[6]

Management Response and Intended Course of Action 1.1

A Project Review Committee was established in 2025 and is comprised of staff from a variety of corporate functions such as ATIPPA, IT, Communications, Access, Records Management and Accessibility. Once senior staff/department heads approve projects, project leads are encouraged to complete a project support form which triggers the Project Review Committee. This process is outlined in procedure on the City's intranet under project management and included in Project Management training in Reach 360.

[6] Please refer to Appendix A for more details on priority levels and a summary of all recommendations categorized by priority.

Conclusion 1.1

Management indicated the recommendations have been implemented.

Action By: Manager, OPS **Action Date:** Complete

Information Only: DCM, Finance & Corporate Services
City Solicitor
City Clerk
Policy Analyst
Policy Equity Associate

Issue 1.2 – Review of Project Review Process by the ATIPP Function

The project review process discussed in Issue 1.1, which was still being developed upon the completion of audit fieldwork, aims to centralize project management at the City and ensure project risks are identified upfront and appropriately mitigated. As privacy risks can have a substantial impact on a project, it is important that the PPIA/PIA process is effectively incorporated into the project review process to mitigate those risks.

Discussions with the ATIPP Analysts at various points in the latter half of 2024 indicated that, although they were aware that a new process was being developed, they had not yet been involved in integrating the PPIA/PIA requirements into it. Since the ATIPP function is responsible for developing and managing privacy procedures for the City, there is a risk that privacy assessments may not be adequately incorporated into the project review process without their input. Consequently, this could lead to unidentified and unmitigated privacy risks for projects.

Recommendation 1.2

The ATIPP function should review the proposed project management review process to confirm it is sufficient in identifying and mitigating project-related privacy risks. As part of this review, consideration should be given to how privacy

impact assessments are incorporated into the process to help ensure their completeness and meet policy and procedure requirements.

Priority Level: P1

Management Response and Intended Course of Action 1.2

The Project Review Committee has been established and both the City Solicitor and an ATIPP Analyst had input into the form and process used to evaluate projects. Both the City Solicitor and an ATIPP Analyst sit on the Committee. This is now in the implementation phase and is currently evaluating projects.

Conclusion 1.2

Management indicated the recommendation has been implemented.

Action By: City Solicitor
Access and Privacy Analysts

Action Date: Complete

Information Only: DCM, Finance and Corporate Services
Manager, OPS

Issue 1.3 – Adopting the Provincial Government's PPIA Process

Documenting business decisions is a critical control as it increases transparency and accountability and creates an audit trail. By establishing a clear audit trail, organizations can help ensure that every decision made aligns with established policies and procedures.

As outlined in City Policy 01-04-02, Privacy Management Policy, the City requires a PPIA to be completed for any project that accesses, collects, uses, discloses, or disposes of personal information. Therefore, all project managers should first evaluate if their project involves personal information to determine if they need to complete a PPIA. If a PPIA is required, the program manager is required

complete a standardized PPIA template and submit it to an ATIPP Analyst for review. As such, the completed template provides documentation that the project includes personal information and that the PPIA process has been completed.

Conversely, program managers may determine that their project does not involve personal information and conclude that a PPIA is not required. In these situations, no documentation is maintained to support the decision not to proceed to a PPIA, and nothing is submitted to the ATIPP Analyst. This differs from what is required under the Government of Newfoundland and Labrador's ("Gov NL") privacy impact assessment process.

Section 72 of the Access to Information and Protection of Privacy Act, 2015 ("Act") stipulates that when a department or branch of the provincial executive government develops a program or service, it must complete either a PIA or a preliminary assessment indicating that a full PIA is not necessary. Therefore, the Act mandates that all projects initiated by Gov NL must complete, at a minimum, a PPIA, regardless of whether the project involves personal information.

An inspection of the Gov NL PPIA template during the audit noted that it allows program managers to skip most sections of the PPIA if their project does not involve personal information. However, the completed template must still be submitted to the applicable ATIPP Coordinator for review and retention. This process is advantageous as it ensures documentation is maintained to confirm that program managers have evaluated whether their projects involve personal information. Consequently, an adequate audit trail is preserved.

In contrast, program managers at the City are not required to document their reasoning for not completing a PPIA, nor do they need to submit any documentation to the ATIPP function to substantiate their decision. This lack of documentation reduces accountability for program managers, which likely contributes to required PPIAs and PIAs going uncompleted at the City.

Also of note is that Gov NL's template includes examples of what constitutes personal information. This guidance helps Gov NL program managers make an accurate determination on whether their project includes personal information. Such information would also be useful on the City's template if the City decides to adopt Gov NL's privacy assessment process.

Additionally, the ATIPPA Review Committee[2] recommended updating the Act during the 2020 statutory review to ensure that section 72 applies to the City of St. John's. Therefore, adopting Gov NL's privacy assessment procedure would align with the stipulations of the Act, which may become applicable to the City of St. John's if the Act is updated as recommended.

Recommendation 1.3

To provide a formal mechanism to document and assess if projects include personal information and require further privacy analysis, management should consider adopting the Government of Newfoundland and Labrador's privacy assessment process as outlined in the Act. This would include:

i. Amending the wording in its privacy assessment procedures to require all new and substantially modified projects to undergo a PPIA or a full PIA.

ii. Updating its PPIA template to allow program managers to bypass the majority of the PPIA if their project does not access, collect, use, disclose, or dispose of personal information.

iii. Updating its PPIA template to define personal information and provide related examples.

Priority Level: P2

Management Response and Intended Course of Action 1.3

Management agrees with the recommendations.

Conclusion 1.3

Management indicated the recommendations will be implemented.

Action By: City Solicitor
Access and Privacy Analysts

Action Date: May 2026

Information Only: City Clerk
Policy Analyst
Policy Equity Associate

Issue 1.4 – Detective Controls

The project review process discussed in Issue 1.1, which was under development when the audit fieldwork concluded, may serve as a preventive control, helping to ensure that projects are evaluated for privacy risks before moving forward. However, preventive controls can fail for several reasons, including human error or unforeseen issues. Therefore, it is generally considered a best practice to implement detective controls in conjunction with preventive measures to improve the overall effectiveness of control processes.

A possible detective control relating to improving the completeness of PPIAs and PIAs could involve having an ATIPP Analyst periodically review a comprehensive list of approved City projects. The goal of this review would be to identify any projects that have not completed a required privacy assessment.

Discussions with the City's Organizational Performance and Strategy Manager indicated that a listing of approved projects at the City could potentially be generated when the project review process is implemented. Depending on the details captured in the listing, the ATIPP Analyst may be able to use it as a tool

for conducting the detective control process, thereby reducing risks related to incomplete privacy assessments.

Recommendation 1.4

To further ensure the completeness of PPIAs/PIAs at the City, the Privacy Analysts should contact Organizational Performance and Strategy management to explore if information can be provided to assist with the implementation of detective controls. Such controls would help identify instances where privacy assessments may be missing or incomplete. One potential detective control could involve a Privacy Analyst periodically reviewing any available listings of projects approved by the City of St. John's to verify that appropriate privacy assessments have been completed for each project.

Priority Level: P2

Management Response and Intended Course of Action 1.4

Office of the City Solicitor

City Solicitor and Privacy Analysts to explore how detective controls can be implemented in conjunction with Organizational Performance and Strategy.

Organizational Performance and Strategy

Organizational Performance and Strategy use a software system called Cascade to manage strategic and other plans. Opportunities exist to create attributes in the system that would allow project leads to note the completion of PPIA/PIA. An account can be provided to ATIPP for monitoring.

Conclusion 1.4

Management indicated that the recommendation will be implemented.

Action By: City Solicitor
Manager, OPS
Access and Privacy Analysts

Action Date: September 2026

Information Only: DCM, Finance & Corporate Services

Issue 1.5 – PPIA and PIA Awareness Initiatives

The Office of the Privacy Commissioner of Canada notes that maintaining an active awareness campaign is part of a well-structured privacy assessment program. Such awareness initiatives, which generally include posters, intranet postings, and email communications, contribute to an increased understanding of PPIA and PIA requirements amongst employees, leading to increased compliance.[7, 8]

Discussions with management during the audit indicated that while all City employees are required to complete comprehensive privacy training, which includes details of the privacy assessment process, launching a privacy assessment awareness campaign could further educate employees and enhance compliance.

Furthermore, the OCIA noted during the audit that the highest number of PPIAs and PIAs completed in a single year was in 2019, coinciding with the implementation of the Privacy Management Policy and its related procedures. This surge can likely be attributed to the PPIA/PIA requirement being top of mind for staff at that time. This reinforces the notion that building awareness for PPIAs and PIAs may reduce compliance-related privacy risks.

[7] Office of the Privacy Commissioner of Canada. (2012). *Getting Accountability Right with a Privacy Management Program.* https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf
[8] Office of the Privacy Commissioner of Canada. (2025). OPC's Guide to the Privacy Impact Assessment Process. https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/

Recommendation 1.5

To increase privacy assessment compliance and further educate City staff on privacy assessment processes, management, in conjunction with the Marketing and Communications Division, should undertake an internal awareness campaign regarding preliminary privacy impact assessments and privacy impact assessments.

Priority Level: P2

Management Response and Intended Course of Action 1.5

City-wide PPIA and PIA training and an awareness campaign for the same are not necessary as only management group staff spearhead projects and complete privacy assessments. The current ATIPP training sufficiently covers the topic for most staff.

The ATIPP Analysts are developing an e-learning module specifically for PPIAs and PIAs that will supplement the Access and Privacy Training and be mandatory for all management group staff. Once developed, awareness messaging will run concurrent to the training period.

In addition, the Privacy Assessment requirement is also supported and reinforced by the Project Review Committee as outlined in Course of Action 1.1.

Conclusion 1.5

Management indicated that the recommendation will be implemented.

Action By: Access and Privacy Analysts **Action Date:** August 2026

Information Only: City Solicitor
Manager, Corporate Communications

Issue 1.6 – PPIAs and PIAs for Current Projects

The Office of the Information and Privacy Commissioner of Newfoundland and Labrador advises that it is best practice to conduct PPIAs/PIAs not only for new or redesigned projects but also for existing ones. However, given resource constraints, assessments for existing projects should be completed as time and resources permit.[9]

Discussions with management during the audit noted that no PPIA or PIA had been completed for any project prior to the implementation of the City's privacy program in 2019. As such, there are long-standing projects at the City, some of which may carry significant privacy implications, that have not completed a privacy assessment.

During subsequent discussions, ATIPP management expressed concerns about the feasibility of conducting assessments for current projects due to limited resources. However, it is important to carry out these assessments to help determine if the City is exposed to any significant privacy risks that should be mitigated. Prioritizing higher-risk projects, especially those that involve sensitive personal information, would be an effective way to optimize resource allocation.

Recommendation 1.6

To help ensure privacy risks are identified and mitigated for current projects, management should:

i. Utilize professional judgment to identify projects implemented before 2019 that likely have significant privacy implications.

ii. As time and resources allow, contact the project owner to initiate the PPIA or PIA process as required.

[9] Office of the Privacy Commissioner of Canada. (2007). *Assessing the Privacy Impacts of Programs, Plans, and Policies.* https://www.priv.gc.ca/en/opc-actions-and-decisions/audits/pia_200710/

Priority Level: P2

Management Response and Intended Course of Action 1.6

Management accepts the recommendations subject to time and resource availability.

Conclusion 1.6

Management indicated that the recommendations will be implemented.

Action By: Access and Privacy Analysts **Action Date:** Ongoing

Information Only: City Solicitor

Issue 1.7 – Project Management Guides

Involving privacy professionals in project management typically results in improved decision-making and outcomes. These specialists can offer valuable insights to identify potential risks and recommend strategies that may be overlooked by those less familiar with privacy requirements.[10]

A project management working group was established at the City in 2018 to foster a common understanding of project management knowledge and ensure adherence to project management best practices. The group consisted of representatives from various City divisions including Organizational Performance and Strategy, Corporate Information Services, Budgeting, Construction Engineering, and Planning, Engineering, and Regulatory Services.

[10] Pahl, C. (2025, January 27). *Lessons for the journey: The evolution of data privacy roles into data governance.* International Association of Privacy Professionals. https://iapp.org/news/a/lessons-for-the-journey-the-evolution-of-data-privacy-roles-into-data-governance

As part of this work, the group created various project tools, templates, and guidance documents for City employees to use when managing projects. One of the main outputs of the group was the Project Management Reference Guide. This comprehensive guide is meant to help project managers execute projects in a controlled manner while mitigating risks, resulting in more effective and quality outcomes.

The Office of the City Internal Auditor reviewed this guide during the audit and noted that it contains detailed guidance on various project areas, including project life cycles, procurement, budgeting, and resourcing. However, the guide does not address privacy considerations for projects or mention the potential need for privacy assessments. The same applies to the Pilot Project Guide found on the City's project management intranet page. Consequently, project privacy risks may not be considered, especially if project managers use these guides as prescriptive guidance when completing City projects.

Subsequent discussions with Organizational Performance and Strategy management indicated that the project management working group was established before the creation of the ATIPP function at the City, as well as before the implementation of the Privacy Management Policy. Consequently, an Access and Privacy Analyst was not available to participate in the working group at its inception, and there was no privacy policy at that time. Management further indicated that the Project Management Working Group is no longer active at the City.

Recommendation 1.7

To ensure that project guidance at the City includes privacy considerations, management should:

i. Review the project management reference guide and pilot project guide to ensure privacy-related best practices for project management are included.

ii. Request that appropriate updates be made to the project management reference guide and pilot project guide, including reference to the PPIA and PIA requirements.

iii. Include an Access and Privacy Analyst in any future project management-related working groups.

Priority Level: P2

Management Response and Intended Course of Action 1.7

Organizational Performance and Strategy

The guide will be removed from the intranet as content has been placed in a Reach 360 course and includes ATIPPA information already. The pilot project guide will be reviewed to determine whether it is required and then updated accordingly. ATIPPA staff are involved in the project review committee and will be considered for any future committees managed through OPS.

Office of the City Solicitor

Management accepts the above recommendations and will assist the Organizational Performance and Strategy Division in their review and updates of project management guidance.

Conclusion 1.7

The Manager of Organizational Performance and Strategy indicated during subsequent correspondence that the recommendations have now been implemented.

Action By: Manager, OPS
Access and Privacy Analysts

Action Date: Complete

Information Only: DCM, Finance & Corporate Services
City Solicitor

Issue 1.8 – Algorithmic Impact Assessments

An algorithmic impact assessment ("AIA") is a best practice risk assessment tool designed to help assess and mitigate the impacts associated with deploying an automated decision system, including impacts related to privacy. An automated decision system includes any technology that either assists or replaces the judgment of human decision makers. Automated decision systems can be used to automate or assist with tasks such as assessing applications for benefits, detecting fraud in financial transactions, and shortlisting job candidates[11].

AIAs are required by the Federal Government of Canada for federal government projects.[12] These assessments were also noted in the 2020 ATIPPA Statutory Review Report[2] from a privacy standpoint. The statutory review report recommends updating the provincial Access to Information and Protection of Privacy Act, 2015 ("Act") to define algorithmic impact assessments and require that any public body planning to implement an automated decision system complete one. Although the Act has yet to be updated as recommended, such revisions could occur during future statutory reviews and related amendments.

[11] Government of Canada (2024). *Directive on Automated Decision-Making.* https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592
[12] Government of Canada (2024). *Algorithmic Impact Assessment Tool.* https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html

Discussions with management and a review of City Policy 01-04-02, Privacy Management Policy, and related procedures, indicated that AIAs are not a requirement at the City, nor are they referenced in any policy or procedure. However, given that AIAs have only recently emerged as an effective risk assessment tool, it is not surprising that their usage has not been adopted by the City. Nonetheless, the absence of these assessments at the City increases the likelihood that risks associated with projects involving automated decision-making may not be mitigated.

Recommendation 1.8

To help identify privacy impacts for projects involving automated decision systems, the City of St. John's should consider:

i. Requiring algorithmic impact assessments for projects that involve automated decision systems.

ii. Updating City Policy 01-04-02, Privacy Management Policy, and its related procedures to reflect this requirement and provide an outline of the algorithmic impact assessment process.

Priority Level: P2

Management Response and Intended Course of Action 1.8

The implementation of the above recommendations is under investigation. Management will meet with Corporate Information Services to determine the applicability of AIAs as a risk assessment tool given the City's current use of automated decision making.

Conclusion 1.8

Management indicated that the recommendation is under investigation. The Office of the City Internal Auditor will assess the implementation status of the recommendation during follow-up audit work.

Action By: City Solicitor
Access and Privacy Analysts

Action Date: August 2026

Information Only: City Clerk
Policy Analyst
Policy Equity Associate

Section 2 – Records Safeguard Plan and Protection of Personal Information

Issue 2.1 – Records Safeguard Plans

The City's Personal Information and Record Protection Procedures stipulate that department heads are responsible for overseeing the development and implementation of a records safeguard plan for their respective departments. This plan is intended to establish appropriate safeguards for departmental records that contain personal information, including electronic records and any records managed by third parties.

To facilitate this process, the ATIPP Coordinator ("ATIPP Analyst") is responsible for providing department heads with a template for the Records Safeguard Plan. Department heads are required to complete the template and return their completed plans to the ATIPP Analyst. The completed plans must include a description of the administrative, technical, access control, and physical safeguards currently in place for departmental records containing personal information. Additionally, they should outline any existing deficiencies in safeguards and the strategies for addressing them.

The City's Archives and Records Management Division ("ARM Division") also play a role in helping safeguard records, as it is responsible for the City's Records and Information Management Procedures. Those procedures include a section titled "Records Security," which states that records and information must be protected from unauthorized access. The procedure also indicates that appropriate physical and technical measures should be applied based on the sensitivity of the information.

Discussions with ATIPP management during the audit noted that while the templates and supporting procedures are in place, the records safeguard plan

process has yet to be completed. However, management suggested that it may be more appropriate for the ARM Division to take on this responsibility.

Management further mentioned that prior discussions between the ATIPP Analysts and the former ARM Manager, who is now the City Clerk, determined that it may be more logical for the records safeguard plans to be housed within the ARM Division rather than the ATIPP function. The reasoning stems from the ARM Division's role in overseeing the protection of all records through its records information management framework. Regardless of the final ownership decision, it is crucial to finalize the records safeguard plans to become compliant with the City's Personal Information and Record Protection Procedures and ensure the proper protection of City records.

Recommendation 2.1

To further safeguard records under the custody of the City of St. John's and ensure procedural compliance, it is recommended:

i. That ATIPP management meet with management from the Archives and Records Management Division to determine which division/function will assume responsibility for overseeing the completion of the records safeguard plan process.

ii. The responsible division/function works with department heads to complete the records safeguard plan process.

iii. To update any associated policy and procedure to accurately outline any change in responsibilities related to the records safeguard plan process.

iv. To revisit the records safeguard plan process periodically to ensure completed plans remain accurate and complete.

Priority Level: P1

Management Response and Intended Course of Action 2.1

Archives and Records Management

The Archives and Records Manager met with the Access and Privacy Analysts on October 21, 2025, to discuss Recommendation 2.1.

The current Records Safeguard Plan focuses on records that contain personal information. The Archives and Records Manager has completed the Records Information Management (RIM) Program draft which will be reviewed by Legal, Audit and Corporate IT Services by November 30, 2025. A key element of the RIM Program recommends that the current Records Safeguard plan be expanded to assess all the City's records (i.e. Information Repository) and highlight all records that are deemed to warrant a completion of a Records Safeguard Template. The RIM Program also acknowledges that the ARM Division assume responsibility for the completion of the Records Safeguard Plan.

The RIM Program Plan will be reviewed by senior management in December of 2025 and will go to council as information in early 2026.

The ARM Division will work with each division to complete a Risk Heat Map (privacy breach likelihood versus impact) for all the City's Information Repository in 2026. Appropriate Records Safeguard Plans will be completed accordingly. The ARM Division will update any associated policy and procedure documentation to reflect the Records Safeguard Plan process.

The ARM Division will review its RIM Program Plan annually to ensure alignment with the City's Strategic Plan is maintained. This will ensure the Records Safeguard Plan process remains current and complete.

Office of the City Solicitor

The Privacy Analysts have had a preliminary discussion with ARM management, and it was agreed that the ARM division would assume responsibility of the records safeguard plan. The Office of the City Solicitor will assist the Archives and Records Management Division as needed in the completion of the records safeguard plan process.

Conclusion 2.1

Management indicated the recommendations will be implemented.

Action By: Manager, ARM
Access and Privacy Analysts

Action Date: Ongoing

Information Only: City Solicitor
City Clerk
Policy Analyst
Policy Equity Associate

Section 3 - Personal Information Banks and Personal Information Inventory

Issue 3.1 – Personal Information Banks and Personal Information Inventory

City Policy 01-04-02, Privacy Management Policy, defines a personal information bank ("PIB") as personal information that is organized or retrievable by either an individual's name, identifying number, symbol, or other unique identifier assigned to the individual. The policy also defines a personal information inventory ("PII") as a comprehensive list of all the City's Personal Information Banks.

Both PIBs and PIIs are also noted in section 111 of the provincial Access to Information and Protection of Privacy Act, 2015 ("Act") under the Publication Scheme. Although this section is not currently applicable to the City of St. John's, the 2020 ATIPPA Statutory Review Report[2] recommended updating the Act to require the creation of publication schemes by all public bodies, except for small municipalities, and to update the schemes every two years. While the Act has not yet been amended to reflect this recommendation, this provision may become relevant to the City of St. John's during future revisions.

Regardless of whether the Act is updated, the City's Privacy Management Policy mandates that the ATIPP Coordinator ("ATIPP Analyst") develop and maintain a PII in compliance with the Personal Information Bank and Inventory Procedures. According to these procedures, each department and its divisions must identify the personal information collections under their custody. Once identified, each division is responsible for compiling a list of its PIBs and submitting them to a Central Department Contact, as designated by the Department Head. The ATIPP Analyst will then work with the Central Department Contact to review the preliminary list. After all departmental PIB listings have been received, the ATIPP Analyst shall consolidate them into a single PII for publication on the City's website.

During discussions with management, it was noted that a personal information bank and inventory project was initiated in 2020. This project resulted in the collection of 49 PIBs across 10 divisions. However, due to resource limitations at that time, the project was not completed. Consequently, additional PIBs still need to be collected, and the compilation of PII remains unfinished. This situation leads to non-compliance with the City's Personal Information Bank and Inventory Procedures. Furthermore, it could pose reputational risks for the city, as citizens may perceive a lack of transparency in how their personal information is being managed.

Further discussions with management indicated that, with the addition of another Access and Privacy Analyst to the ATIPP function since the project's inception, it may now be feasible to complete the project. Doing so will help mitigate the previously noted risks.

Recommendation 3.1

To ensure compliance with City Policy 01-04-02, Privacy Management Policy, and related procedures, management should:

i. Initiate a personal information bank and inventory project that would result in an accurate and complete personal information inventory for the City of St. John's.

ii. Once all the PIBs have been collected and reviewed, management should:

    a. Compile a personal information inventory.

    b. Work with the Marketing and Communications Division to develop a personal information inventory webpage as part of the City's website.

c. Post the personal information inventory on the City's website.

d. Update the personal information inventory, at least, every two years.

Priority Level: P1

Management Response and Intended Course of Action 3.1

Management accepts the above recommendations.

Conclusion 3.1

Management indicated the recommendations will be implemented.

Action By: Access and Privacy Analysts **Action Date:** October 2026

Information Only: City Solicitor
Manager, Corporate Communications

Section 4 – Governance

Issue 4.1 – Policy, Website, and Form Updates

It is an accepted best practice to ensure that information included in organizational policies, procedures, forms, and websites is accurate. This accuracy helps ensure that consistent business processes are carried out and stakeholders, including the public, can rely on that information for decision-making purposes.

A review of City Policy 01-04-02, Privacy Management Policy, during the audit noted that it was approved by Council on June 25, 2019. While most of the policy is still accurate, it has not yet been updated to reflect the City Manager as the newly designated head of the public body. Similarly, a review of the PIA template, the City's website, and selected public-facing privacy forms still lists the City Clerk as the head of the public body and/or has the ATIPP function reporting to the Office of the City Clerk.

Since the City of St. John's Council only approved the change in the head of the public body in September of 2024, it is understandable that such documents have yet to be updated. However, these inaccuracies increase the risk that stakeholders, such as employees or citizens, may rely on incorrect information.

Recommendation 4.1

To ensure that the City Manager is properly recognized as the new head of the public body and to address other changes arising from the recent adjustments to the reporting structure for the ATIPP function, management should collaborate with the Policy Analyst to review and update City Policy 01-04-02, Privacy Management Policy, as well as the related procedures, forms, and the City's website.

Priority Level: P2

Management Response and Intended Course of Action 4.1

Management accepts the above recommendation.

Conclusion 4.1

Management indicated the recommendation will be implemented.

Action By: Access and Privacy Analysts **Action Date:** May 2026

Information Only: City Solicitor
City Clerk
Policy Analyst
Policy Equity Associate

Issue 4.2 – Formal Mandate Letter

As highlighted in the 2020 ATIPPA Statutory Review Report[2], it is a good practice for the ATIPP Coordinator ("ATIPP Analyst") to be issued a formal mandate letter signed by the head of the public body. The letter should set out the responsibilities and authority of the ATIPP Analyst and outline the public body's commitment to achieving the objectives of the provincial Access to Information and Protection of Privacy Act, 2015 ("Act"). The report also recommends posting the mandate letter on the public body's website and preparing a new mandate letter as personnel changes.

Related discussions with management indicated that such a letter has not been prepared for the City's ATIPP function. In less mature ATIPP functions, this could create risks associated with inconsistencies and inefficiencies. However, audit procedures conducted throughout the audit demonstrate that the City's ATIPP function is well established and staffed by competent personnel who understand their roles and responsibilities.

Instead, preparing and posting an official mandate letter on the City's website would enhance the transparency and accountability of the City's privacy

processes. It would also allow the City to formally document its commitment to protecting citizens' personal information and complying with the provisions of the Act.

Recommendation 4.2

To formally document the City's commitment to achieving the objectives of the Access to Information and Protection of Privacy Act, it is recommended that:

i. The City Manager, as the designated head of the public body for the City of St. John's, draft a formal mandate letter to the ATIPP Analysts, who serve as the Coordinators, outlining the City's commitment to achieving the objectives of the Act and related roles and responsibilities of those involved.

ii. Post the mandate letter on the City's website to improve transparency and accountability.

Priority Level: P3

Management Response and Intended Course of Action 4.2

Management accepts the above recommendations.

Conclusion 4.2

Management indicated the recommendations will be implemented.

Action By: City Manager **Action Date:** March 2026

Information Only: City Solicitor
Manager, Corporate Communications
Access and Privacy Analysts

Appendix A

The Office of the City Internal Auditor assigns a priority ranking to each recommendation. These rankings offer guidance to management on the significance of each recommendation and how to prioritize its implementation/consideration among all recommendations in the report.

P1 recommendations require immediate management attention and should be prioritized first for implementation. P2 recommendations should be implemented in the near term but are less urgent than P1 recommendations. P3 recommendations are the least urgent among all recommendations and can therefore be prioritized last for implementation.

The table below summarizes all the recommendations from the Privacy Management Review, categorized by their priority level for implementation.

Recommendation	***Priority 1***	***Priority 2***	***Priority 3***
1.1 - Project Review Process	✓		
1.2 - Review by the Access and Privacy Function	✓		
1.3 - Adopting Gov NL's Process		✓	
1.4 - Detective Controls		✓	
1.5 - PPIA and PIA Awareness Initiatives		✓	
1.6 - PPIAs and PIAs for Current Projects		✓	
1.7 - Project Management Guides		✓	
1.8 - Algorithmic Impact Assessments		✓	
2.1 - Records Safeguard Plans	✓		
3.1 - PIBs and PII	✓		
4.1 - Policy, Website, and Form Updates		✓	
4.2 - Formal Mandate Letter			✓