Audit of the Toronto Police Service's Information Technology Governance

Driving Improved Accountability and Transparency in Achieving Technology Objectives

May 4, 2026

Tara Anderson, CPA, CA, CFE, CIA, BAcc
Auditor General

AUDITOR GENERAL TORONTO

Table of Contents

Executive Summary 1

Background 8

Audit Results 12

A. Improving the Information Technology Governance Framework 12

A. 1. Need for an Enterprise Risk Management function to track, monitor, and report on technology risks 13

A. 2. Management reports to the Board do not provide a consistent and holistic overview of planned and in-progress technology projects and initiatives 15

A. 3. TPS's technology strategy needs strengthening, and the Board's Strategic Plan is to be finalized 20

A. 4. Technology-related policies and procedures are not up to date 22

B. Enhancing Data Governance, Privacy, and Information Security 26

B. 1. Improve Project Management with timelier remediation of Privacy Impact Assessment findings 26

B. 2. A consistent user access management review process, to support data governance and security, is not in place 28

B. 3. Need to establish a dedicated approach to information and data governance to improve data quality and promote a culture that safeguards private and sensitive information 30

B. 4. Enhancing the mandate of the Chief Information Security Officer 31

B. 5. Need for structured reviews of vendor security and control reports to ensure TPS data is well safeguarded 33

C. Other Operational Governance Improvements 35

C. 1. Persistent technology vacancies increase risk of project delays and control gaps 35

C. 2. Officer training on appropriate use of artificial intelligence (AI) tools and related controls should be rolled out promptly 36

Conclusion 38

Audit Objectives, Scope and Methodology 40

Appendix 1: Management's Response to the Auditor General's Report Entitled: "Audit of the Toronto Police Service's Information Technology Governance" 42

Executive Summary

The Auditor General's 2025 Work Plan included an audit of Information Technology (IT) governance at the Toronto Police Service (TPS). This audit examined the TPS's approach to IT governance, an area of significant importance given the TPS's use of technology to deliver policing services to support their mission: to keep Toronto the best and safest place to be.

Why this audit matters

The TPS is currently undergoing major transformations in the technologies it uses to deliver policing services to the people of Toronto. Strong governance and oversight are essential to support effective management of technology and successful transition to new IT systems.

Audit objectives

The overall objective of this audit was to assess whether the TPS has an IT Governance Framework in place to guide the organization in supporting its mission and strategy. The audit aimed to answer:

1) Does the TPS follow a formal IT Governance Framework aligned with its mission and values which promotes accountability, transparency, and informed decision making?

2) Is a prioritization process followed for selecting IT Projects, and how they are managed, monitored, and overseen to stay on track?

3) Do operational oversight processes exist for IT Operations, Cybersecurity, and other technology areas?

TPSB motion related to highlighting matters on data governance and privacy in the Auditor General's report

Towards the end of our audit fieldwork, the Toronto Police Service Board (TPSB, or the Board) passed a motion at its March 4, 2026 Board meeting[1] asking that our audit highlight matters related to data governance and privacy in this report which may inform the Board's oversight in light of Project South.[2]

[1] Toronto Police Service Board Meeting | March 4 Meeting Minutes (pages 5 and 7)
[2] Project South is a 2025-2026 anti-corruption investigation led by York Regional Police related to multiple TPS officers accused of leaking confidential database information to organized crime figures.

Data governance and privacy were already included in the scope of this audit at a high level. The Auditor General has made five recommendations in **Section B** of this report that directly relate to improving data governance and privacy. The other 10 recommendations relate mainly to strengthening IT governance, including enterprise risk management and reporting on technology projects/initiatives, which will also complement improvements to data governance and privacy.

What we found

Improvements made by the TPS to improve IT governance

The TPS has taken steps to improve its IT governance over the past decade, such as hiring a Chief Transformation Officer (CTO) and Chief Information Security Officer (CISO), development of an IT benefits framework, standardization of IT project management practices (including a framework for selecting and prioritizing IT projects), and establishing a data management unit. We found that further work remains to mature and formalize the TPS's IT Governance Framework. This report highlights areas for continued improvement under the following three broad categories:

- Improving IT Governance Framework
- Driving improved privacy and data governance
- Other operational governance improvements

A – Improving IT Governance Framework

1. Need to establish an Enterprise Risk Management function to improve IT governance

ERM is needed to ensure high risk IT areas are prioritized, addressed and monitored by the TPS and Board

An Enterprise Resource Management (ERM) function helps organizations and their Boards to identify and monitor enterprise risks, including IT risks. Risk management is an important component of an effective IT Governance Framework, so that the IT risks evaluated as the highest risks are prioritized, addressed, and monitored. We found that an integrated ERM function is not currently in place at the TPS.

Consistently tracking and reporting enterprise-wide risks, including those related to IT, is crucial to better inform decision making at both the TPS and the Board level.

2. Management reports to the Board do not provide a consistent and holistic overview of planned and in-progress technology projects and initiatives

Improve consistency and frequency of reporting to Board on technology projects and initiatives, including important risks

The TPSB would benefit from receiving regular reporting on the status of in-progress and planned technology projects. Updates on the status of major IT projects, and enterprise-wide projects that include IT, are done on an ad hoc basis and do not provide details on some of the important risks the projects are facing, such as delays which can increase costs.

More consistent and frequent reporting, using dashboards and easy to understand templates is needed to keep the TPSB apprised of the status of major technology initiatives and projects.

3. TPS's technology strategy needs strengthening, and the Board's Strategic Plan is to be finalized

Board staff have advised that the TPSB is currently finalizing its Strategic Plan, which will provide governance direction for the TPS to develop and implement a technology plan. A Technology Plan will help the Board in holding the Police Chief (the Chief) and the TPS accountable for achieving objectives related to technology, outlining the reporting the Board requires, and will also help better inform the Board on how they can further support and allocate resources within the TPS to help achieve its technology-related objectives and priorities.

The TPS has an IT benefits framework which helps to provide some high-level direction related to technology. However, a more detailed plan on technology is needed, which will need to be aligned with the Board's upcoming new Strategic Plan.

4. Technology-related policies and procedures are not up to date

11 of 39 sampled technology-related policies not updated in over 10 years

The TPS and the TPSB need to strengthen their processes related to reviewing and updating technology-related policies. We found 11 out of 39 sampled technology-related policies had not been updated in over 10 years, despite some of these having an internally specified requirement for annual reviews or updates. For example, the Information Security Master policy has not been updated in over 11 years.

28 of the 39 technology-related policies also did not specify an internal timeline for when they should be subject to review. It is important to keep all policies up to date, particularly those that are critical to the TPS's ongoing operations, to ensure compliance and consistency in practices.

B – Enhancing Data Governance, Privacy, and Information Security

1. Improve Project Management with timelier remediation of Privacy Impact Assessment findings

A Privacy Impact Assessment (PIA) is performed to identify privacy risks when implementing new IT systems and technologies, or when upgrading existing IT systems where personally identifiable information (PII) is processed.

Addressing risks from PIAs before systems go live

Although the TPS has performed PIAs, validation that all recommendations resulting from PIAs have been addressed is not always done or documented before systems go live. For five systems which held personal data, documentation was not available to determine that all PIA findings were addressed before the systems were put in production.

PIA recommendations should all be addressed before systems go live, or alternatively, acceptance of any residual risks should be documented and approved by an appropriate executive leader as the risk owner.

2. Need for a consistent user access management review process, to support data governance and security

Regular user access reviews not performed

While the TPS has established controls over granting initial access to its IT systems, the controls need to be strengthened where TPS members[3] change roles, move across departments/divisions or leave the organization. The TPS does not regularly perform a user access review.

A periodic user access review is an important control to help ensure that users only retain access to the IT systems and sensitive data they require to perform their jobs, and that when members leave the TPS or have a change in their roles, the access is deactivated in a timely manner.

[3] The term used by TPS for individuals in its workforce, whether uniformed officers or civilian, is "member," and is used throughout the report.

3. Need to establish a dedicated approach to information and data governance, to improve data quality and promote a culture that safeguards private and sensitive information

Dedicated approach to information and data governance is needed

The TPS does not have formally designated data governance roles across the enterprise, such as data custodians, data owners, and data stewards. The TPS has initiated work to improve data governance through its Information Management Framework, however more work is needed to strengthen accountability and security of sensitive data. The Auditor General has recommended a dedicated approach to information and data governance, including controls that will help to improve the TPS's protection of data privacy, as well as improve its data quality.

4. Enhancing the mandate and resources of the Chief Information Security Officer

CISO needs direct access to key security information sources and reports

Our review of the CISO's function at the TPS indicates that this role needs both the appropriate resources and mandate to perform and fulfill its assigned responsibilities. For example, the CISO needs direct access to key security information sources and reports, as well as adequate resources and authority to develop and enforce security policies and controls at the TPS. This will help the CISO to address timely remediation of cybersecurity risks as they arise over time.

It is also important for the CISO to have the ability to provide independent reports on the status of cybersecurity to executive leadership[4] on a periodic basis, and for the Chief to then present those reports to the TPSB, supported by the CISO.

5. Need for structured reviews of vendors' security and control reports to ensure TPS data is well safeguarded

The TPS makes use of third-party vendors who handle sensitive data. It is critical to assess whether these vendors maintain adequate controls in their systems and processes to protect TPS information and data.

TPS does not regularly review vendors' security attestation reports

The TPS does not regularly review vendors' security attestation reports and therefore does not flag or follow-up on the findings reported in these reports. For example, we noted in two of the three vendors' security attestation reports reviewed that the TPS was not aware of security risks identified in these reports that required addressing by the vendors.

[4] In this report, "executive leadership" refers to the most senior leadership officers (the level of Director and Chief Superintendents or higher) within the TPS focusing on primarily strategic matters. "Management" refers to general leadership including line managers as well as owners of system and services, with a general focus on operational matters.

C – Other Operational Governance Improvements

1. Persistent technology vacancies increase risk of project delays and control gaps

Delays in filling IT positions - Vacancies of 25-40 positions over past 5 years

Over the past five years, the number of vacancies in the TPS's IT Services unit has ranged from 25 to 40 positions within the approved headcount, resulting in vacancy rates of 14 to 20 per cent (refer Section C.1, Table 3).

Management advised that funding for some of these unfilled positions was reallocated to operational areas. Filling the key vacant technology positions will be important to be able to ensure the foundational controls in IT are strengthened and that the recommendations in this report are implemented.

2. Officer training on appropriate use of artificial intelligence (AI) tools and related controls should be rolled out promptly

Developments related to AI tools require ongoing vigilance

The Board issued its policy on artificial intelligence in 2022, with its last update in 2024. With the rapid spread and speed of advancement of AI, the TPSB's policy on AI should be subject to a shorter review cycle.

The AI policy should also be sufficiently flexible to consider different use cases for AI tools and provide the TPS with the ability to assess these technologies through a different lens when being applied in non-policing administrative uses, leveraging a risk-based approach. In addition, given that AI tools are rapidly evolving, training for members on the responsible use of AI needs to be rolled out promptly and should be mandatory.

Conclusion

Overall, the TPS has partially implemented the functions assessed in the three objectives of this audit, and further work is needed to strengthen IT governance at the TPS. The recommendations in this report will help further mature and strengthen the TPS's approach to IT Governance.

TPS IT Governance Framework needs to be strengthened and formalized

With respect to the first audit objective, the TPS needs to formalize its IT Governance Framework to further strengthen accountability and transparency. This includes establishing an Enterprise Risk Management function including IT risks, consistent and holistic reporting on technology projects and initiatives to the Board, strengthening its technology strategy and aligning it with the Board's Strategic Plan, and updating and regularly reviewing technology-related policies and procedures.

TPS needs to address privacy impact assessment findings before IT systems go live

In relation to the second objective on technology project management, while TPS has developed a framework for IT project selection and prioritization, project management and reporting on in-progress and new projects require strengthening. Improved processes are needed to ensure identified privacy risks from Privacy Impact Assessments are addressed before IT systems go live.

Lastly, the third audit objective pertained to operational oversight of technology areas. With regards to data governance and privacy, the Auditor General has made several recommendations to improve controls in this area across the TPS, including consistent and regular user access reviews and enhancing the mandate of the Chief Information Security Officer to strengthen information security. The TPS will need to ensure that there are adequate resources, including timely filling of vacant technology positions, to support these functions. In addition, AI policies and tools need to be updated more frequently and training provided.

Implementing the 15 recommendations contained in this report will further improve the work that has been initiated by the TPS and TPSB, improving IT governance, and further strengthening IT controls, including data governance and privacy.

Thank you

We express our appreciation for the co-operation and assistance we received from the Chief, Command, and TPS members, and the board members and staff of the TPSB.

Background

In December 2019, the Toronto Police Service Board requested the Auditor General to complete a risk assessment of the TPS and develop a risk-based audit plan.[5] This plan, which was independently developed by the Auditor General, established TPS priority areas when auditing risks. The audit of IT governance was included in the audit plan and was in the Auditor General's 2025 Work Plan.

IT governance refers to the structured framework that guides how organizations strategically manage and optimize technology to support and achieve business objectives and deliver value, while mitigating risks. Strong IT governance includes the following practices which help to drive positive outcomes:

Strong IT Governance Practices

- Enterprise Risk Management function which helps management to establish an Enterprise Risk Management framework to identify, prioritize, track, and address risks, including technology risks, in order to achieve the organization's objectives. This also better informs the Board to help them in their oversight role with prioritization and decision making, including the allocation of resources.
- Regular and holistic reporting to the Board on technology projects and initiatives, providing sufficient information on the status and important risks, which supports accountability, transparency and informed decision making, to support the organization in achieving its technology objectives.
- A Technology Strategy or Plan that aligns with the organization's mission and values, and provides direction and oversight for the organization to ensure technology is supporting the effectiveness and efficiency of its operations.
- Technology-related policies and procedures are regularly reviewed, updated, and enforced to ensure that clear direction is provided and that practices of members are in compliance with regulations.
- Operational oversight processes and strong controls exist for data governance and privacy, IT operations, cybersecurity, AI, and other technology areas.

[5] Auditor General's Risk Based Audit Plan of the TPS

Technology supports the operations of the TPS

The TPS is the largest municipal police force in Canada,[6] with a net operating budget of approximately $1.2 billion,[7] and 8,200 members, including 5,400 police officers.[8]

The IT budget included $113 million in operational expenditures for 2025, and expected IT-related capital spending of $497 million is planned over the next ten years.

The TPS has five main organizational areas, internally referred to as "Commands"[9]. Deputy Chiefs oversee different elements of policing operations, and civilian leaders oversee administration and the technology and transformation supporting operations. The five Commands are:

1. Corporate Services Command – under the Chief Administrative Officer
2. Technology & Transformation Command – under the Chief Transformation Officer (CTO): **the main focus of this audit**.
3. Community Safety Command – representing all police Divisions
4. Specialized Operations Command – comprised of various speciality and investigative squads such as Public Safety Operations and Detective Operations
5. Operations Support Command – including Field Services, the 9-1-1 and non-emergency call centres operated by Communications Services, Parking and Traffic, as well as Investigative Support, among others

Organizing delivery of policing through six service lines

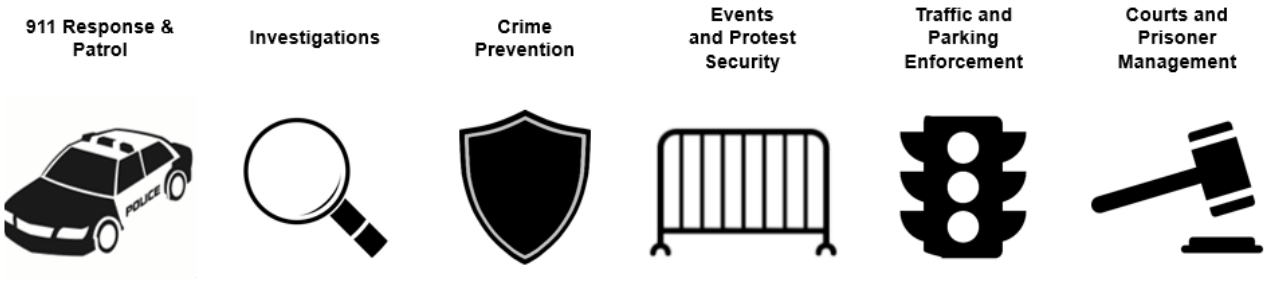
The TPS has organized the delivery of its policing operations through six service lines, as shown in **Figure 1** below. Management is creating roadmaps for each of these service lines to outline their responsibilities and make it easier for the public to understand the TPS's work. The roadmaps will also help guide and prioritize support functions, including technology and other administrative units.

Management advised that future reporting to the Board may also align with the structure of these service lines.

---

[6] Statistics Canada - Municipal police services serving a population of 100,000 or more, Canada, 2019
[7] 2025 Budget Notes - Toronto Police Service
[8] 2024 - Toronto Police Service - Chief's Annual Report, page 8 – note that parking enforcement officers and volunteer auxiliaries are not included
[9] With respect to the TPS hierarchy, reporting to the Commands are "pillars," which are led by directors or Chief Superintendents. Each pillar is composed of areas and units under them.

Figure 1: Service Lines of the Toronto Police Service

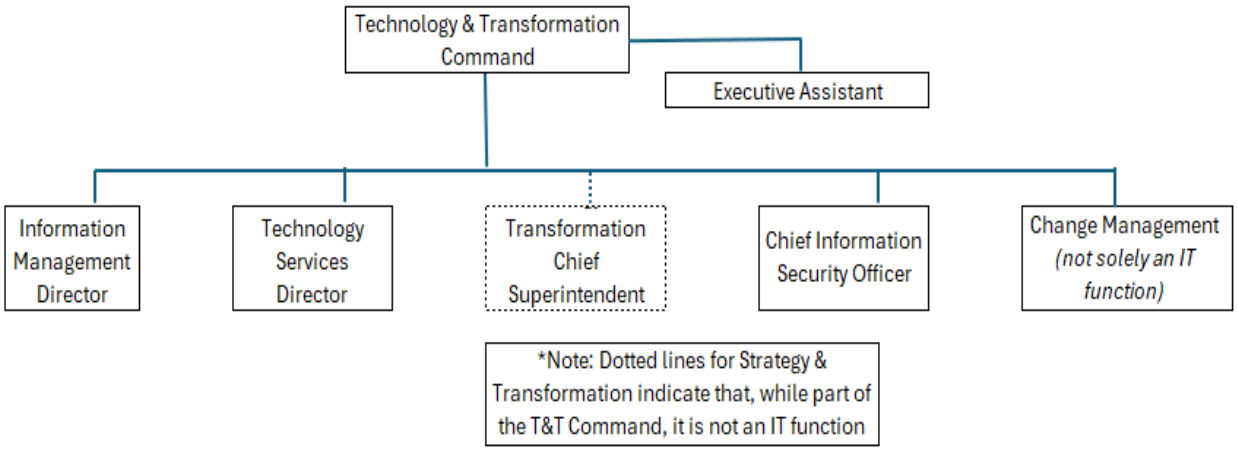


Technology & Transformation Command

Major technology functions reporting to the CTO

The primary focus of this audit was on the TPS technology functions within the TPS, such as information technology services, information management, and cybersecurity. These functions are performed by several areas in the Technology & Transformation Command and report to the CTO. **Figure 2**, below depicts the organization of the CTO's pillar.[10]

Figure 2: CTO's Pillar Organization Chart Excerpt



Key functions depicted above (from left to right) include:

- Information Management (IM), which focuses on managing TPS data, Information Security, and data analytics support.

[10] The Intelligence Services unit operates its own IT functions outside of the direct purview of the CTO, and was not a focus of the audit due to the sensitivity of its operations.

- Information Technology Services (ITS), which performs IT help desk support, manages technology projects, and supports development and operation of business and policing applications. It is also responsible for maintaining organization-wide IT project standards, governance, and best practices.

- Although an IT Risk Management unit exists under the ITS Director, its focus on risk is limited as the dedicated resource hired to address technology risks is on a long-term secondment to support the Fédération Internationale de Football Association (FIFA) World Cup 2026 tournament preparations.

- The Strategy and Transformation unit, although not primarily an IT-related function, reports to the CTO on both strategic transformation as well as equity, inclusion & human rights matters.

- The CISO, with responsibility for the TPS incident response plan, reporting on compliance to established security baseline standards, and coordinating independent cyber security testing.

- The Change Management unit (previously known as Business Relationship Management) handles both IT and non-IT related organizational change matters.

Audit Results

A. Improving the Information Technology Governance Framework

Information Technology (IT) governance refers to the structured framework that guides how organizations strategically manage and optimize technology to support and achieve business objectives and deliver value. In this report, when we refer to IT , we are broadly referring to technology, which also includes functions related to information management and security, and data governance, among others.

Over the past decade, the TPS has taken several actions to improve its IT governance. These actions include:

- Hiring a Chief Information Officer, now the Chief Transformation Officer (CTO)
- Hiring a Chief Information Security Officer (CISO)
- Development of an IT Benefits Framework
- Improving standardization of IT project management practices, including a framework for selecting and prioritizing IT projects
- Establishing a Data Management unit

Further work remains to mature and formalize the TPS's IT Governance Framework

Further work remains to mature and formalize the TPS's IT Governance Framework. An improved and formalized IT Governance Framework, together with improvements made through implementing our recommendations in this report, will assist executive leadership and the TPSB in improving accountability and transparency, including reporting on progress in achieving the TPS' objectives related to technology, and further informing decision making related to technology projects and initiatives.

Recommendation:

1. **The Board request the Chief of Police, Toronto Police Service, to formalize and document an IT Governance Framework which should include and address the recommendations made in this report.**

A. 1. Need for an Enterprise Risk Management function to track, monitor, and report on technology risks

Consistently and holistically tracking and reporting enterprise risks is an important element of governance and helps manage technology risks. It provides the Board and executive leadership with awareness of major technology risks and how they are managed and mitigated to achieve the organization's goals.

The TPS has not established an Enterprise Risk Management (ERM) function or framework, in order to have an integrated ERM tracking and reporting process to evaluate technology risks across the organization. This issue was also raised by the TPS's internal audit function in its *2018 Corporate IT Risk Management* report. While the TPS previously had a Corporate Risk Management pillar, it disbanded following a re-organization that took place approximately five years ago.

While some individual TPS units and sections track risks within their own areas, risks are not consolidated or viewed holistically across the organization. This increases the likelihood that some issues may not receive sufficient attention for risk mitigation.

No central TPS risk management function in place to consolidate and identify systemic issues

Risks are not being assessed and documented consistently, since each individual risk rating system follows its owners' interpretation of risk, rather than being overseen by a central TPS-wide risk function. It is also possible that the individual risks, when combined, may pose a larger risk and/or could point to systemic issues.

Consolidating the enterprise-wide risks will help executive leadership identify, track, and monitor technology risks, including mitigation plans and status. This will help ensure risks are managed and mitigated properly; prioritization is performed; resource use is optimized; and better information is provided to support decision making.

When an ERM function is being implemented, it will be helpful for executive leadership to determine the level of risk appetite and tolerance it accepts for enterprise risks, including those related to technology with the Board. This will enable executive leadership to ensure enterprise-wide risks do not exceed the organization's risk appetite or tolerance.

Examples of technology risks not currently reported on a regular basis

Examples of some of the enterprise-wide risks related to technology which may warrant periodic reporting to the Board and executive leadership include:

- Cybersecurity risks related to critical IT systems at the end of their vendor supported life
- Technology project delays, or other significant risks, which may delay gaining new efficiencies or other expected benefits, or leading to higher costs than planned
- Reporting on risks of unaddressed Privacy Impact Assessment findings, increasing the risk of unauthorized disclosure of personal information
- Data governance and privacy related risks, such as risks from user access control reviews and monitoring exception logs for unusual or unauthorized access
- Technology obsolescence risks (patching or upgrades to unsupported technology systems), including business continuity risks
- Succession planning risks, including the effects of unfilled IT vacancies

Technology risks are currently provided to the Board on an ad hoc and siloed basis. It is important for the Board to receive regular updates on enterprise-level risks, including technology risks, and mitigation plans, to help Board members perform their duties.

Comprehensive ERM and reporting will help identify areas for improvement as risk mitigation plans are put into practice, and help in overseeing transformational projects to ensure they are performing well. It will also help with identifying risks, to address them in a timely manner to support delivering expected strategic value, on budget, and in accordance with planned timelines.

Recommendation:

2. The Board request the Chief of Police, Toronto Police Service, to develop and implement an Enterprise-wide Risk Management (ERM) framework, which includes:

a. Identifying and tracking enterprise-wide risks, including technology risks

b. Developing risk tolerance in consultation with the Board, and criteria for evaluating risks on their impact and likelihood

c. Reporting on a regular basis to the Board and executive leadership on major IT risks and their mitigation plans, including any risks that cannot be mitigated or managed to an acceptable level in the required timeframe.

A. 2. Management reports to the Board do not provide a consistent and holistic overview of planned and in-progress technology projects and initiatives

The existing reports updating the Board on technology projects are ad hoc in frequency and do not provide sufficient information for the Board to be fully apprised of the complete picture of the organization's status with respect to technology projects.

Existing capital variance reporting does not provide sufficient insights on technology matters to TPSB

Management primarily reports on technology projects to the TPSB through capital variance reporting, as well as ad hoc technology project updates. Capital variance reports are primarily financial in nature and only provide a description of certain individual technology projects. These reports are not meant to provide a holistic overview of all technology initiatives or flag potential issues for follow-up and further review.

Capital variance reports are also "re-baselined"[11] at the start of every year. This means only a portion of larger longer-term initiatives are presented to the Board, which increases the difficulty of tracking ongoing challenges and longer-term delays on certain projects.

The TPS is currently working to deliver potentially high-impact transformational technology projects, which need consistent reporting and timely oversight. For example, the largest transformational technology project underway is the replacement of the TPS's Records Management System (RMS), used by over 5,000 TPS members. The new system is expected to retire several legacy systems and will affect the TPS's key operations, from priority police response to 9-1-1 calls, to prisoner management, as well as evidence handling, and support for criminal investigations and prosecutions. The reporting on the RMS project is used as an example below of how reporting to the TPSB needs to be further improved.

Example - overview of plans for the Records Management System Project

As summarized in **Table 1**, the budget for the RMS project has undergone several revisions in both cost and timeline for delivery.

[11] Variance reports reset progress against the year's budget and targets, which resets the status of projects which would have been over or under performing at the end of the previous reporting year.

Table 1: RMS – Project Cost Overview

Funding request/stage	Project Budget	Timeframe for Delivery and Completion
2022 Initial funding placeholder[12] (Included in 2023-2032 Capital Program Request presented at January 2023 TPSB meeting)	$20.6 million[13]	2023-2024 (Management advised completion was expected in two years from the point of initiation[14])
2023 Business Case (As per contract award presented at April 2023 TPSB meeting)	$30.6 million[15]	2023-2025
Q4 2025 Capital Variance Report 2025 Year End Status (Presented at April 2026 TPSB Meeting)	$29.3 million[16]	2023-2028[17]
Capital budget and plan for 2026-2035 (Presented at December 2025 TPSB Meeting)	$35.7 million[18]	2023-2027

Initial Plans for the RMS Project

The initial funding placeholder request for the RMS as presented in January 2023 as part of the TPS 2023-2032 Capital Program Request was $20.6 million, indicating the project would be expected to be completed in two years.

[12] The $20.6 million amount was presented as an initial funding placeholder request against the TPS capital reserve.
[13] Toronto Police Service 2023-2032 Capital Program Request, page 18
[14] Project initiation occurred with a kickoff meeting with the vendor on February 20, 2024.
[15] TPSB Meeting – April 28, 2023, page 181
[16] Capital Budget Variance Report as at December 31, 2025, page 140 – the project's budget was temporarily reduced through an "in year transfer" to fund another project, the Real Time Operating Centre project. This does not represent an actual change to the project, as TPS Finance expects the funds will be transferred back in 2026.
[17] Capital Budget Variance Report as at December 31, 2025, page 142
[18] Preliminary 2026-2035 Capital Program budget – this is the current state of the RMS project's total expected cost.

Contract award and update to the RMS budget allocation and project's timeline

In March 2023, TPS prepared a vendor contract award and a detailed business case for TPSB approval, totalling $30.6 million. This included a revision to the timeline, moving the planned project end date to 2025, and included a $5 million contingency budget. The variance reporting format is not designed to carry forward this important information regarding changes from prior year timeframes and amounts.[19]

Contingency fees not included in initial funding request

Half of the RMS project's increased budget allocation to $30.6 million was attributed to setting a $5 million contingency. Contingencies for IT projects are a common practice to address unexpected changes, and the preliminary estimate would have benefited from also including a contingency amount. The TPS should ensure that future system planning and discovery work includes a contingency amount at the earliest point of allocation to the capital plan, rather than adding it on to the cost of a project at a subsequent step in the Board approval process.

As of October 2025, the entire $5M contingency budget has been allocated to be used in completing project development, so there is no remaining contingency available to draw upon if needed.

Variances between the 2026-2035 RMS capital budget request and the Q4 2025 capital variance report

The 2026-2035 capital budget request presented to the Board on December 8, 2025 indicated that the total RMS project cost would be $35.7 million. The $5.1 million increase to the total budget was identified as the expected cost of training and additional licences for new TPS members. Training costs are typically included earlier in the budgeting process for large technology projects. The additional cost of $5.1 million was not reflected in the capital variance report as of Dec 31, 2025 presented to the TPSB in April 2026.

The project was expected to go live in 2027, however the Q4 2025 Capital Variance Report cited in **Table 1**, indicates a revised 2028 project end date.

[19] The request to increase the RMS budget included these elements: support for backfill, analytics and training, licensing and maintenance costs, increased quantity of licenses due to an increase in the number of users, and setting up a contingency budget

Consistent reporting on projects' progress needed

Infrequent updates to the TPSB regarding the status of major technology projects

The last major Program Update to the Board on the status and milestones of RMS was in June 2025.[20] Consistent and more frequent reporting on its status, including advance warnings of any major risks or obstacles to timely and successful deployment, is critical to help the project avoid experiencing more delays, given the high profile and impact of this project.

Some Board members have advised us they do not feel well briefed on the status of technology projects, including the reasons for delays, which timelier and more frequent reporting to the Board would help address.

Status reporting for technology projects and initiatives needs more consistency and detail

Without regular and consistent reporting and status updates, the Board and executive leadership will lack full awareness of the status of all technology projects and potential delays and other obstacles facing technology initiatives.

Use a consistent template or dashboard showing progress on all technology initiatives

Key elements to consider when improving reporting include using a consistent template or dashboard showing progress on all technology initiatives to easily compare results over time, including progress made to address previously identified risks. Reports should present original and revised timelines for long-running projects to help gauge progress over time and help determine if additional resources or time are required, or to document the reasons for changes in expected scope and benefits.

Coordination of consolidated reporting on transformational or operational projects with significant technology component

There is no coordination of consolidated reporting to Board on operational projects with a significant technology component

There is also a need to improve the coordination of consolidated reporting to the Board on transformational or operational projects that have a significant technology component. For example:

- Facilities reporting on the remaining work related to commissioning the TPS's new Data Centre, and
- Deployment of the Mobile for Public Safety (MPS) system, a new technology to support tracking officers' whereabouts.[21]

[20] Although interim variance updates and a 2026 budget request update did cite the status of RMS at a high level, these did not constitute an update on milestones to the Board from the RMS project team itself, which the June 2025 update indicated would be reported in Q1, 2026.

[21] This example relates to the rollout of the MPS system, which replaced the Mobile Data Terminal, and was previously targeted for a February 2025 rollout. The MPS did not go live until November 2025, and the associated risks that materialized and led to this delay were not clearly communicated to the Board. The MPS is an important supporting system for the RMS, and adds a key benefit in offering a "one-push button" feature, to allow for easy recording of officers' arrival times at a call for service.

In the above examples, the owners are from the business units, and reporting to the Board generally has a focus on operational concerns and less on technology risks. The TPS should leverage the existing project management function to operate at an enterprise-wide level to coordinate with the owners of projects that cover more than one pillar or service line, including projects with significant technology components, and provide consolidated project status reporting on a regular basis to the Board.

Reporting on expected benefits of technology projects

The TPS's technology projects are expected to provide benefits, which may include savings, efficiencies, and service improvements in police operations. However, where challenges arise and/or there are delays or increased costs, the anticipated savings and efficiencies may not be realized in a timely manner, or to a lesser degree than planned. The loss or delay of anticipated benefits should be included in projects' ongoing reporting to the Board on the status of expected savings or benefits.

Earlier involvement of the Board in technology decisions

The Board should be involved earlier in long-term technology planning

It is a good practice for the Board to be involved early in decisions related to future contract renewals for upgrades or replacements of major IT systems. We found that the Board is generally not briefed on such initiatives during the preliminary planning stage – new systems like the AI-powered Toronto Non-Emergency Tool (TNET)[22] are announced once selected rather than subject to an advance planning discussion. Involving the Board earlier will allow the Board to be better informed when making long term planning decisions and the related allocation of resources.

Recommendations:

3. **The Board request the Chief of Police, Toronto Police Service, to leverage the existing project management function, to serve at an enterprise-wide level, to help coordinate with the owners of projects that cover more than one pillar or service line, including projects with significant technology components, and provide consolidated project status reporting on a regular basis to the Board.**

[22] TNET is being operated using a technology called HyperAI, to deliver a new AI-driven voice triage system designed to assist callers on the non-emergency line.

4. **The Board request the Chief of Police, Toronto Police Service, to develop a clear and easy to understand technology reporting package for the Board to be provided on a regular basis. The reporting package should include a consistent template or dashboard providing:**

   a. **Status of progress on meeting timelines, budget and expected benefits on technology projects, including any revisions from the original budget and timelines**

   b. **Baseline metrics to help measure benefits following the introduction of new or enhanced systems**

   c. **Challenges impacting the implementation and mitigation strategies for risks**

   d. **An outlook, including longer-term, of planned major technology investments, including future upgrades, rationalizations, replacements, projects, and new technology initiatives.**

A. 3. TPS's technology strategy needs strengthening, and the Board's Strategic Plan is to be finalized

An IT strategy provides an organization with a documented plan on how it aims to use technology to achieve its business objectives. A good IT strategy includes the organization's key priorities and goals, any required resourcing, and key actions needed to achieve its intended goals. The TPS has an IT Benefits Framework, developed to guide transformative efforts by identifying the expected benefits from the current technology programs and projects that are underway. However, the IT Benefits Framework does not include certain strategic elements such as key performance indicators, an approach to technology risk treatment, and the approach to be taken to manage internal resources through talent management. There is also no detailed plan aligned to this framework to help management achieve the strategy outlined.

Police Service Boards have several important oversight responsibilities, per Ontario's *2019 Community Safety and Policing Act* (the CSPA, or *the Act).*[23] The CSPA requires that Boards create a strategic plan, which must address several topics, including Information Technology.

[23] Community Safety and Policing Act, 2019, section 38-39.

Per the CSPA, the Chief of Police is accountable for setting and achieving the established objectives and timelines, and for reporting back to the Board on progress on policing activities, and technology projects and initiatives. The TPSB's Executive Director has advised us that the Board's Strategic Plan is under development and is expected to be finalized in Q2, 2026.

TPSB has an important IT Governance oversight role to perform

An important oversight role for the Board is to hold the Chief accountable for achieving the TPS' objectives related to technology, which are in support of police operations. In interviews, some Board members noted that they do not receive sufficient insights into the strategic direction of IT for the TPS. They attributed this in part due to the lack of consistent and regular reporting on the status of technology matters to the Board.

Even if Board members do not have technical IT expertise, communication can be provided in a way that enables them to be well informed and to make key decisions on IT investments and strategic direction for the TPS. The Board would benefit from engaging with the Chief and CTO to articulate and agree on a consistent way to report on the selection and adoption of new technologies in support of the TPS's overall policing strategy and objectives.

The Board's strategic plan should include governance direction for the TPS to develop and implement a technology plan and an Enterprise Risk Management framework to help the Board in holding the Chief and the TPS accountable for achieving objectives related to technology and outline the reporting the Board requires. This will help better inform the Board on how they can further support and allocate resources within the TPS to help achieve its technology-related objectives and priorities.

As emergency service providers, police organizations and their Boards need to consider how their IT systems support achieving effective and efficient operations, including answering and responding to 9-1-1 calls for service and other important policing duties and responsibilities.

Importance of ensuring sufficient investment in IT systems and staffing

It is not uncommon for organizations providing emergency services to prioritize funding for frontline delivery and for technology to not necessarily receive the full funding required. However, sufficient investment in IT systems and staffing is required to ensure the organization has strong IT controls as well as reliable IT systems that support effective and efficient operations.

Over time, the TPS's IT systems will reach end of life and require upgrades or replacements. While management has established an Enterprise Architecture outline which serves for more granular work on technology development, the Board needs to be involved at the outset of high-level planning when considering potential strategic technology project and procurement decisions such as system replacements.

Recommendations:

5. **The Auditor General recommends that the Board ensures its Strategic Plan provides governance direction for the Toronto Police Service to develop and implement a Technology Plan and an Enterprise Risk Management framework, to hold the Chief and the TPS accountable for achieving its technology objectives and outlining the reporting on technology matters required by the Board.**

6. **The Board request the Chief of Police, Toronto Police Service, to strengthen its Technology Strategy to include:**

    a. **Key performance indicators in relation to IT benefits framework**

    b. **Approach to technology risk treatment**

    c. **A process to assess the organization's alignment between the Toronto Police Service Board's Strategic Plan and the objectives set by the Toronto Police Service to deliver technology.**

A. 4. Technology-related policies and procedures are not up to date

As a law enforcement organization, it is very important for the TPS to keep its technology-related policies and procedures up to date, so that members comply with the current direction and regulations expected of them.

The technology-related policies and procedures serve an important role in governing police operations. They act as fundamental tools to translate strategies into daily operations and ensure consistency, accountability and transparency across the organization. For full effectiveness, policies and procedures must be regularly reviewed and updated.

Significant number of policies have not been reviewed during their assigned review cycle

Although the TPS has policies and procedures to help guide technology operations, they are not updated or reviewed regularly, despite some requiring annual review. Out of 39 technology-related policies[24] reviewed, we noted:

- 11 policies were more than 10 years old, including two critical foundational policies requiring annual reviews[25]
- Over 10 different TPS policies did not have an assigned owner
- 28 of the sampled policies did not indicate a timeline for being reviewed and updated[26]

A detailed list of policies requiring an update was provided to management. Below are examples of some key technology policies in need of review.

[24] 34 of the 39 tested policies are internal to the TPS, and 5 of the 39 tested policies are owned by the TPSB
[25] Of the policies aged over 10 years, 10 are TPS policies, and 1 is a TPSB policy
[26] 2 TPSB and 26 TPS policies did not specify a review cycle

Table 2: Examples of Key TPS Policies Requiring Updates

Policy/ procedure name	Description and comments	Last updated	Time elapsed since last update
Information Security Master Policy	Intended to maintain a technology environment to protect TPS information resources and data, including personally identifiable information (PII) of service members and citizens. The policy's scope covers all information assets. Controls apply to anyone who has access to business data or systems that store or process data. The document states it should be reviewed annually.	September, 2014	11+ Years
Database, Email and Test Data Security Policy	Defines the standards of protection for sensitive data on all TPS databases, email systems, and production environments. The policy requires that the systems in scope are protected and subject to annual security reviews.	March, 2015	11+ Years
TPS Operations Security Policy	Defines security requirements to: • Safeguard servers, mobile computing devices and storage media • Provide accountability and malware protection • Ensure continued availability of critical information resources. The scope of this policy covers all TPS information assets, mobile computing devices, servers and workstations. The document states it should be reviewed annually.	January, 2015	11+ Years
Vendor Remote Access Policy for Production Environments	Defines the processes governing remote access to TPS production systems by third party vendors; links to a 16 year old access request template, rather than pointing to the newer internal TPS IT ticketing system.	May, 2014	11+ years
Infrastructure Lifecycle Management	Defines and identifies infrastructure assets within the TPS such as servers, storage, networking, data centres, etc. It details the planning, procurement, deployment and management of these infrastructure assets.	November, 2019	6 Years

Although the TPS has a public service procedure library, there is a need to develop a comprehensive unit-specific[27] index of policies which pertain to IT and security related matters. An index will help track and perform file reviews, and to update or discard technology policies as appropriate.

Importance of keeping policies up to date

Ensuring that technology-related policies, including those related to information and cybersecurity, are updated according to their defined review cycle (often annual) reinforces a strong "tone at the top". Out-of-date documentation presents the risk of not being in alignment with the current organizational IT strategy or not providing sufficient clarity or consistency.

Outdated documentation may also result in unclear direction around IT decisions, including how to apply old policies with current technologies. Other risks stemming from not updating technology policies and procedures include:

- Members may ignore policies if they feel they are not relevant due to not being updated regularly or enforced
- Not complying with current laws and regulations
- Lack of clarity and guidance for TPS members on how to comply with Information Security rules
- Guidance not updated to include new or emerging cybersecurity risks, which can increase the risk of security or data breaches
- Inconsistent practices impacting organizational culture as policies are outdated, not encouraged, or not followed

Ensure policies are being reviewed or updated in a timely manner

The TPS does not follow a consistent process to oversee and manage technology policies and ensure policies are being reviewed or updated in a timely manner, nor a standard template for technology policies and procedures exists. We also found several technology policy documents without clear ownership and responsibility to maintain them.

Recent departures of members, temporary transfers to other roles, and internal reorganization may have contributed to the lack of timely updates. The IT governance team, which could have performed these functions, was disbanded approximately five years ago due to reassignments and retirements.

[27] The functions under the Chief Transformation officer have their own policies governing operations within their unit.

Technology policies are also important in relation to supporting data governance and information security; technology policies must be updated regularly to make it easier for members to look up related information: for example, the Information Breach policy, last updated in 2023, refers to the TPS Information Security Policy and other resources, but the associated hyperlinks point to invalid internal links.

A separate recommendation for the Board for updating policies has also been added under recommendation #15.

Recommendation:

7. The Board request the Chief of Police, Toronto Police Service, to implement a process for managing the review and update of technology policies, to include:

a. Creating an index for IT policies and procedures

b. Ensuring that all technology policies have clearly assigned owners and review frequency timelines

c. Performing a regular review to update policies according to their established timelines.

B. Enhancing Data Governance, Privacy, and Information Security

B. 1. Improve Project Management with timelier remediation of Privacy Impact Assessment findings

New technologies with privacy considerations need stronger control and oversight

A Privacy Impact Assessment (PIA) helps management identify risks and impacts that new or existing systems may have on individuals' privacy. PIAs help ensure compliance with legislative and policy requirements, identify security gaps, and reduce the risk of improper or unauthorized collection, use, disclosure, retention, and disposal of personal information.

As per the guidance of the Office of the Privacy Commissioner of Canada[28], PIAs, including potential privacy impacts, should be addressed before a system goes live and problems could occur.

[28] Office of the Privacy Commissioner's Guide to the Privacy Impact Assessment Process

We found that PIA risk acceptance documentation and treatment plans are not consistently recorded and tracked. Management advised that this is due to insufficient assigned members to perform this function, and the lack of an established regular follow-up process and controls to halt implementation of new IT systems before risk treatment plans are completed or accepted as open risks.

Stronger controls and oversight needed over remediation of PIA findings

Although technology project management practices were recently updated with standardized templates, a structured intake process, and more consistent internal status reporting within the IT unit, the project management framework and practices can be further strengthened. In particular, this will ensure timely actions are taken on risks identified in PIAs before a system goes live.

A common practice in technology project management is to use key milestones (Project Stage Gates) as checkpoints to ensure risks, including PIA findings are addressed prior to the go-live date.

Undocumented or incomplete PIA remediation activities

Some examples of PIA recommendations that were not completed or documented as 'addressed', before systems went live include:

- Ensuring data retention periods are set when redacting video evidence and other personal information
- Ensuring controls are in place to assess security of evidence handling systems
- Conducting threat risk assessments for certain systems before they are put to production
- Updating procedures for handling of personal information
- Delivering training to service members to ensure they are familiar with handling personal information
- Setting up controls over automatic data retention and deletion

The lack of assigned ownership for the outstanding items has resulted in an accountability gap in completing these activities. This underscores the importance of ensuring follow up on overdue PIA remediation activities.

Ensuring new technologies and supporting procedures have consistent reporting and oversight related to privacy

The Board has an important role to play when the TPS considers using new and emerging technologies, or applying existing technology in new use cases that may introduce new privacy risks. Board oversight should include asking the Chief whether new technologies or services requiring PIAs are being considered, such as electronic memo books or new use cases for drones.

Recommendation:

8. **The Board request the Chief of Police, Toronto Police Service, to strengthen its Project Management Framework to ensure:**

   a. **Privacy impact assessments are performed for all technology projects including new technologies involving personal data**

   b. **Results of privacy impact assessments are recorded and tracked for addressing risks**

   c. **Where privacy risks categorized as high or medium are not fully mitigated before the system's go-live date, a formal risk acceptance describing compensating controls should be signed by the risk and project owners, including the Chief Information Security Officer, the Chief Transformation Officer, and, where appropriate based on the level of risk being accepted, the Chief of Police**

   d. **The privacy risks which are categorized as high and not fully mitigated are reported to the Board and executive leadership.**

B. 2. A consistent user access management review process, to support data governance and security, is not in place

We noted that the TPS does not currently have a regular user access review process in place, to periodically assess whether members' access to systems is appropriate and ensure access is modified or deactivated promptly when no longer required. Without a regular user access review, there is an increased risk of users' access not being removed in a timely manner, which increases the risk of sensitive data sets and networks being accessed inappropriately.

Complex organization with high turnover has increased risk of errors in removing user access in a timely manner

Timely user access reviews are important when users may have access to sensitive data in a large organization. This is especially relevant at the TPS, with over 180 specialized units, and in light of the recent alleged leaks of confidential information by TPS members identified as part of Project South. This will remain an important area to address as the TPS introduces new IT systems, implements its five-year hiring plan, and the ongoing possibility of unit re-organizations and changes to individual members' roles.

The TPS's technology policies mandate that access to systems should be limited to only users requiring that level of access. Periodic user access reviews are an important control for organizations to validate the level of access granted to its users and determine if the access continue to remain appropriate, when members have a change in their roles, or have left the TPS to ensure their access is deactivated in a timely manner. Periodic access reviews are also an important element of data governance, helping to restrict access to sensitive information.

Given the criticality of data and systems at the TPS, an annual attestation from all members and contractors on maintaining confidentiality of data and systems will further strengthen data governance and privacy.

Recommendation:

9. The Board request the Chief of Police, Toronto Police Service to strengthen data governance and privacy by implementing a process to:

a. Perform periodic reviews of user access profiles with respect to assigned roles and the required level of access to data and IT systems

b. Deactivate user access where such access is not needed

c. Obtain annual attestation from all TPS members and contractors, to remind them of their obligations under their Oath or Affirmation of Office, to comply with policies related to accessing and maintaining required privacy of confidential data and systems.

B. 3. Need to establish a dedicated approach to information and data governance to improve data quality and promote a culture that safeguards private and sensitive information

Defining data governance

The City of Toronto defines information and data governance[29] "*as the exercise of authority, control, and shared decision-making (accountability, planning, monitoring, and enforcement) over the management of information and data, to ensure authenticity, integrity, and usability of information and data throughout their lifecycles, according to legislation, policies, and best practices.*

Information governance is driven by legal, business, and compliance requirements, while aligning with strategic and operational goals and objectives.

Data governance is often seen as a subset of information governance, focusing on the integrity, storage, and lifecycle management of structured data assets. Effective data governance is a key component of information governance."

TPS has started initial work on data governance

The TPS has begun addressing some elements of data governance with its Information Management Framework, which can be further improved by leveraging the City of Toronto's Information and Data Governance policy.

The TPS also established a Data Management unit approximately a year ago, which is pursuing improved data quality standards and supporting open data initiatives. These data governance activities are still developing. There are no formally designated data governance roles for data owners, custodians, and stewards to oversee the administration and quality of data.

Frameworks such as ISO/IEC 38505[30] and COBIT 5[31] also have guidance on how to implement data governance. These should be considered in conjunction with guidance on privacy from the Office of the Privacy Commissioner of Canada, which outlines 10 fair information principles, including Accountability and Safeguards.[32]

A dedicated privacy-focused approach to data governance will align data management at the TPS with best practices in data governance, including controls such as:

- Safeguarding sensitive records by reviewing a register of access, identifying the members who access these records

[29] City of Toronto Information and Data Governance Policy
[30] ISO/IEC 38505 is the International Organization for Standardization' publication on data governance
[31] The Control Objectives for Information and Related Technologies (COBIT) framework, version 5, is ISACA's framework for IT governance and management
[32] PIPEDA fair information principles - Office of the Privacy Commissioner of Canada

- Recording justifications for accessing data (e.g., supporting a system that automatically ties data record retrieval to general occurrences, the TPS term for a police record created to record information about a person and incident – the new RMS could automate this activity for records accessed in conjunction with its use, to simplify the task of identifying higher risk occurrences of data access).
- Ensuring security is in place for the safe custody, transport, and storage of data, and implementation of additional rules as required.
- Ensuring data retention schedules are consistently defined and rolled out across the TPS for its various IT systems.

Recommendation:

10. The Board request the Chief of Police, Toronto Police Service, to:

a. Take a dedicated approach to data governance which establishes data owners, stewards, and custodians to oversee data quality and security, to address the areas for improvement identified in this report

b. Develop and provide training for members to ensure they understand their responsibilities for securing data under their control and maintaining the required privacy for it.

B. 4. Enhancing the mandate of the Chief Information Security Officer

The CISO's scope of work has grown commensurately with the increased complexity and scale of IT. In general, CISOs develop cybersecurity policies, align cybersecurity strategies and overarching business goals, and lead the organization's work to address cyber threats.

Our review of the TPS CISO's function indicates that this role needs both the appropriate resources and mandate to effectively perform its assigned responsibilities. Currently, the CISO has only one assigned position, to be filled, and limited control over IT security and related governance functions.

Cybersecurity-related reporting to the Board is limited, as the CISO does not regularly report on the status of TPS's cybersecurity posture. To ensure independence and effectiveness of this function, in many organizations the CISO reports to a leadership position outside of IT or to the head of the organization itself.

Stronger CISO role will support timely remediation of cybersecurity risks

A stronger CISO role will help in advancing the maturity of cybersecurity governance and ensuring cybersecurity risks are addressed in a timely manner as new threats emerge over time.

Areas where the CISO requires additional support include:

- A mandate to consistently report on the status of security matters to the Chief and the Board.
- Standardized and expanded information sharing and access (e.g., ensuring the CISO can directly access threat intelligence, the security operations centre, and the IT inventory and risk tracking system)
- Oversight or access to information security unit's reports to help gather information, develop or take ownership of security policies, and address identity and access management issues.
- Formal consultation milestone points in the technology intake and project development processes requiring CISO approval and input on cybersecurity matters.
- Oversight and leadership on cybersecurity awareness activities, including owning existing and future exercises such as phishing campaigns.
- Ensuring sufficient security controls and guidance are in place to guard against accidental data loss/breach deliberately or via emerging technology such as artificial intelligence prompts.
- Reviewing critical security policies and procedures implementation, such as, results of user access reviews to sensitive applications, data governance etc.

The CISO does not own important security-related activities, such as developing and enforcing security policies, including data governance, to ensure TPS members only have the minimum required level of IT access to systems and data based on their role and operational needs. The risk of sensitive information in TPS IT systems being breached has the potential for serious harm and reputational damage.

Recommendation:

11. The Board request the Chief of Police, Toronto Police Service, to review the current mandate and resources assigned to the Chief Information Security Officer; the review should include:

- **a. Independence of the role of the Chief Information Security Officer with respect to organizational reporting structure**
- **b. Adequacy of resources to develop and implement cybersecurity policies across the Toronto Police Service**
- **c. Direct access to the necessary cybersecurity information and reports generated across the organization**
- **d. Mandatory involvement in projects and initiatives that require a cybersecurity perspective**
- **e. Providing regular reports to executive leadership and the Board on the status of cybersecurity risks across the organization**
- **f. Taking ownership of cybersecurity training and education such as, social engineering awareness training and phishing tests.**

B. 5. Need for structured reviews of vendor security and control reports to ensure TPS data is well safeguarded

Vendors present an emerging risk area for organizations, when technology systems and other services are outsourced to third parties that may hold personal or sensitive data, or interact with TPS systems.

Vendor attestation reports, such as System and Organization Controls (SOC) 2 reports, provide assurance for the clients, stakeholders, and related users of a service organization that the vendor's services operate under a set of controls that support security, availability, processing integrity, confidentiality, and privacy.

The SOC 2 and related reports are generally provided by vendors annually. Management is expected to operate its own process for regularly reviewing these reports from vendors, however this is not taking place at the TPS.

TPS management does not regularly review SOC 2 reports to assess their content. Without a standard review process or a dedicated resource to regularly review SOC 2 reports and perform follow-ups on exceptions and gaps, this important task is not being performed. Unmitigated risks in vendors' security environments represent risks to TPS data and systems.

Issues found in two of three tested vendor security reports

We noted issues in two of the three third party security reports we reviewed, which were not investigated by management until prompted by our audit. One security report contained a qualified opinion – which is a negative audit conclusion. The vendor subsequently provided clarification to management regarding the issues in this SOC 2 audit report. The second report had findings; however, management did not follow-up to determine if the exceptions were related to the TPS environment.

Increased focus needed on external vendor attestation

As the TPS engages in trials and pilots with new vendors and service providers, it should ensure it collects and reviews SOC 2 and other related cybersecurity audit and attestation reports early on in the process. It is important to assess new vendors during the initial test and pilot phases to ensure that security considerations are addressed prior to widespread adoption.

Third party vendor relationships are established with different units within the TPS. The TPS should develop a vendor attestation review process to ensure a consistent approach is taken when reviewing these reports.

Recommendation:

12. The Board request the Chief of Police, Toronto Police Service, to establish a process to review vendors' cybersecurity attestation reports regularly to determine whether:

a. Vendors' services remain certified or attested under industry recognized standards

b. Cybersecurity weaknesses identified in the attestation reports are addressed by the vendors, where possible

c. Where weaknesses identified in the attestation reports have not been addressed by the vendors, to validate that risks to the TPS data and systems are assessed, and that non-compliance is addressed according to contractual obligations.

C. Other Operational Governance Improvements

C. 1. Persistent technology vacancies increase risk of project delays and control gaps

In reviewing the Information Technology Services unit headcount, we noted that vacancies in 25 to 40 positions (see **Table 3**) have persisted over the past five years. Management advised that several factors contributed to the gaps, including talent scarcity, competitive salaries in the private sector, long onboarding times, the need to backfill roles following internal promotions and transfers, and challenges in passing security clearance.

IT management advised us that the causes for delays in filling vacancies and the average time to hire are not readily available or tracked. As a result, we were unable to include this information in our audit. It is important to understand the root cause for the delays in hiring and to better manage the hiring process and the workforce going forward.

We found that in cases of retirements, leaves of absence and long-term secondments of IT staff that we reviewed, these remained unfilled for five months or more after their departure. These include positions dedicated to addressing IT risk and updating technology policies (two important areas identified in **sections A.1** and **A.4**), which were repurposed for other operational activities.

If IT members are not replaced or hired in a timely manner, it can negatively impact technology projects and controls. Project-specific tasks may be delayed if there is an excessive gap between the departure and replacement dates, which can impact completion, targeted deadlines, and performance of assigned tasks.

Table 3: History of IT Vacancies – Figures per Management

	Approved IT positions	Actual IT staffing	Variance to approved positions	Vacant Positions as % of approved positions
2021	183	158	25	**14%**
2022	188	154	34	**18%**
2023	187	160	27	**14%**
2024	202	162	40	**20%**
2025	205	172	33	**16%**

Delays in filling IT staffing vacancies also reduces the opportunity for knowledge transfer and results in additional time spent on training of the role that is being taken over.

Recommendation:

13. **The Board request the Chief of Police, Toronto Police Service (TPS), to review existing hiring practices, particularly for IT positions, to:**

    a. **Develop and formalize criteria for reporting on long outstanding vacancies, reasons for delays, and their impact on operations**

    b. **Identify tasks and processes that hinder filling of vacancies in a timely manner**

    c. **Review hiring lead times, target turnover and vacancy levels, and revise processes where needed to address delays in completing the hiring of IT positions in a timely manner**

    d. **Identify IT positions of highest risk to be prioritized and resourced in selecting vacancies to be filled.**

C. 2. Officer training on appropriate use of artificial intelligence (AI) tools and related controls should be rolled out promptly

Artificial intelligence (AI) tools (including large language models such as ChatGPT and other AI) have greatly risen in prominence and their use continues to proliferate globally. Unfettered use of AI tools introduces issues related to maintaining the confidentiality of personal and sensitive information. To address these issues, organizations have introduced policies to manage AI use until the technology has been properly assessed to address the risks of errors that AI tools may introduce.

The TPSB's *Use of Artificial Intelligence Technology*[33] policy articulates how AI tools should be used by TPS members. The policy states that "Service Members may not use new AI technologies prior to receiving approval and training in accordance with the procedure(s) and process(es)." This policy is supported by an internal TPS order, which requires approval from the CTO before use of any new technology is permitted.

[33] TPSB: Use of Artificial Intelligence Technology

The current AI policy does not distinguish between the use of AI tools for operations, such as policing activities, and internal productivity tools, used for non-criminal investigative office work. The TPS AI policy was developed in 2022, prior to the widespread adoption of easily accessible AI tools, and currently mandates a review once every three years. Given the rapid evolution in AI tools, the policy should be reviewed more frequently.

Rapid introduction of new AI features necessitates additional controls

Software vendors have been introducing new AI features in their software, complicating efforts to control access to AI tools. The TPS has limited technical controls to prevent TPS members from using unauthorized AI tools and does not actively monitor access to these tools by TPS members. The TPS needs to develop more comprehensive IT controls over access to these tools to ensure members are using AI tools appropriately and according to policy.

Importance of training on use of AI tools for members

Although under development, there is also currently no mandatory training for members on the responsible use of AI tools. AI tools are rapidly evolving in their capabilities and nature. While the use of unauthorized AI tools is not permitted, there is a need to expand on training and implementation of controls concerning their use.

Recommendations:

14. The Board request the Chief of Police, Toronto Police Service, to:

a. Explore the feasibility of implementing technical controls to monitor, control, or block access to unauthorized AI tools where needed

b. Ensure that mandatory training, including ongoing refreshers, on responsible use of AI tools is rolled out for all Toronto Police Service members.

15. The Auditor General recommends that:

a. The Board ensure a process is implemented to update Board policies in a timely manner

b. The Board update the AI Policy to include consideration of non-policing uses of AI in addition to policing uses, and that the policy be subject to a shorter review cycle.

Conclusion

The TPS is in the midst of major technological transformations expected to streamline its policing processes. As the TPS relies on technology to coordinate the activities of over 8,000 TPS members, effective IT governance is critical.

Overall, the TPS has partially implemented the functions assessed in the three objectives of this audit and further work is needed to strengthen IT governance at the TPS. The recommendations in this report will help further mature and strengthen the TPS's approach to IT Governance.

TPS IT Governance Framework needs to be strengthened and formalized

With respect to the first audit objective, the TPS needs to formalize its IT Governance Framework to further strengthen accountability and transparency. This includes establishing an Enterprise Risk Management function including IT risks, consistent and holistic reporting on technology projects and initiatives to the Board, strengthening its technology strategy and aligning it with the Board's Strategic Plan, and updating and regularly reviewing technology-related policies and procedures.

The TPS needs to address privacy impact assessment findings before IT systems go live

In relation to the second objective on technology project management, while the TPS has developed a framework for IT project selection and prioritization, project management and reporting on in-progress and new projects require strengthening. Improved processes are needed to ensure identified privacy risks from PIAs are addressed before IT systems go live.

Lastly, the third audit objective pertained to operational oversight of technology areas. With regards to data governance and privacy, the Auditor General has made several recommendations to improve controls in this area across the TPS, including consistent and regular user access reviews and enhancing the mandate of the CISO to strengthen information security. The TPS will need to ensure that there are adequate resources, including timely filling of vacant technology positions, to support these functions. In addition, AI policies and tools need to be updated more frequently, with training provided.

15 recommendations to improve IT governance

Implementing the 15 recommendations in this report will help the TPSB and TPS improve its IT governance and improve the transparency and accountability in achieving its technology-related objectives.

Thank you

We express our appreciation for the co-operation and assistance we received from the Chief, Command, and TPS members, and the board members and staff of the TPSB

Audit Objectives, Scope and Methodology

The Auditor General included the IT governance audit of the TPS in her 2025 Work Plan.[34]

Audit objectives

The overall objective of this audit was to assess the extent to which the TPS has an IT Governance Framework in place to support the TPS's mission and strategy. This audit aimed to answer the following questions:

1) Does the TPS follows a formal IT Governance Framework aligned with its mission and values, which promotes accountability, transparency, and informed decision making?

2) Is a prioritization process followed for selecting IT projects, and how they are managed, monitored, and overseen to stay on track?

3) Do operational oversight processes exist for IT operations, cybersecurity and other areas?

Audit scope

IT governance audits represent an assessment of overall IT governance structures at a point in time. For this audit, it represents the state of IT governance at the TPS and TPSB in 2025 to April 2026.

Areas not covered within the scope of this audit

This audit did not review disaster recovery policies and procedures in detail, as this was being currently assessed by TPS internal audit. This audit also did not perform detailed testing of IT operations, and did not include governance over other City of Toronto divisions' or agencies' IT systems which interface with the TPS (e.g., The Toronto Parking Authority's Green P application, and the Toronto Fire and Toronto Paramedic Services' 9-1-1 systems).

Audit methodology

Our audit methodology included:

- Interviews with members and staff of the TPSB to collect insights and an understanding of the reporting process and structures
- A high-level review of governance processes over IT operations

[34] Auditor General's Office 2025 Work Plan and Budget Highlights – Section A.2, Table 1, Page 8

- Interviewing members from the TPS's technology-related business units, including project managers, directors, and members of executive leadership
- Reviewing IT governance structures, frameworks, budget information, policies and procedures, risk management artefacts, minutes of TPSB meetings, and reporting to key stakeholders
- Reviewing a sample of technology-related policies and procedures
- For two large technology projects - reviewing project specific records, such as business cases, requests for proposal, steering committee meeting minutes, project RAID[35] logs, and materials reported to the TPSB
- Examining vacancy statistics and historical staffing levels within the IT unit
- Inspecting and reviewing third party vendors' audit and attestation reports
- Conducting other procedures that were deemed relevant.

Sampling methodology

We judgmentally selected 34 TPS and five TPSB IT policies and procedures for detailed review. These samples were selected based on factors such as operational importance, elapsed time since review, knowledge of technology shifts, and the criticality of the policy to the TPS.

We also judgmentally selected two technology projects based on identified risks for further review. Factors followed in making these samples selections included project value, project risk, operational and strategic importance, and data sensitivity.

Compliance with generally accepted government auditing standards

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[35] A RAID log is a project management tool that tracks "risks, assumptions, issues, and decisions."

Appendix 1: Management's Response to the Auditor General's Report Entitled: "Audit of the Toronto Police Service's Information Technology Governance"

Recommendation 1: The Board request the Chief of Police, Toronto Police Service, to formalize and document an IT Governance Framework which should include and address the recommendations made in this report.

Management Response: ☒ Agree ☐ Disagree
Comments/Action Plan/Time Frame: TPS agrees with this recommendation. As part of the Board's forthcoming Strategic Plan, the Board has committed to establishing direction for the Service's efforts to modernize technology and infrastructure, within the stated goal of increasing community safety in both fact and perception. This direction will allow the Service to modernize technology to ensure residents can access services more easily, receive faster and more consistent support, and better understand how the Service is performing. The Service will follow the Board's direction to implement a Technology Plan (including an IT Governance framework) that aligns with existing operational frameworks and planning processes, including the Community Safety and Well-Being Operational Roadmap, the Service Line operating model, and Information Management's Analytics Framework. Under the direction of Chief Transformation Officer Colin Stairs and the Command Team, the Service will ensure the Auditor General's recommendations are considered while creating this plan. An implementation timeline will be developed once a foundational plan is in place; current estimate is implementation by 2029.

Recommendation 2: The Board request the Chief of Police, Toronto Police Service, to develop and implement an Enterprise-wide Risk Management (ERM) framework which includes:

a. Identifying and tracking enterprise-wide risks including technology risks

b. Developing risk tolerance in consultation with the Board, and criteria for evaluating risks on their impact and likelihood

c. Reporting on a regular basis to the Board and executive leadership on major IT risks and their mitigation plans, including any risks that cannot be mitigated or managed to an acceptable level in the required timeframe.

Management Response: ☒ Agree ☐ Disagree
Comments/Action Plan/Time Frame: TPS agrees with this recommendation in principle. Implementation is dependent upon obtaining appropriate budget and resource allocations to support. As part of the Board's forthcoming Strategic Plan, the Board has committed to overseeing the

development and implementation of an Enterprise Risk Management (ERM) framework to proactively identify, assess, monitor and mitigate risks. This is one of the activities identified to achieve the Board's stated priority of transparent and trusted governance. The Service will support ERM implementation in a number of ways, including:

- Strengthening internal processes to identify, assess, monitor and report on both organizational and community safety, including risks related to technology
- Building a clearer connection between governance oversight and measurable public safety outcomes by linking risks identified within the 6 Service Lines and linking those risks to the harms policing is intended to prevent, reduce or disrupt
- Strengthening internal governance practices, including internal accountability and reporting mechanisms, to ensure consistency with legislative and other standards (e.g. ISO 38500 [Governance of IT for the organization])
- IT Risk unit within Information Technology Services (ITS) will continue documenting IT risks and mitigations in the Enterprise Architecture State Management (EASM) repository, enhancing the reporting on high-priority risks, and securing full-time risk management resources to support the ERM initiative
- IT Risk will continue to dedicate a full-time equivalent resource to ensuring support and alignment with the Board and Service's overall ERM framework, following the completion of FIFA World Cup activities
- Information Management (IM) will integrate its risk-related practices into the ERM so that IM issues with a residual risk rated high are provided for review and reporting

The Service has committed to supporting the establishment of ERM processes that align technology, operational and community safety risks with Board requirements. Exact timelines will be developed once the implementation team has been resourced and funded; current estimate is implementation by Q4 2028.

Recommendation 3: The Board request the Chief of Police, Toronto Police Service, to leverage the existing project management function, to serve at an enterprise-wide level, to help coordinate with the owners of projects that cover more than one pillar or service line, including projects with significant technology components, and provide consolidated project status reporting on a regular basis to the Board.

Management Response: ☒ Agree ☐ Disagree
Comments/Action Plan/Time Frame: TPS agrees with this recommendation. Implementation is dependent upon obtaining appropriate budget and resource allocations to support. The Service recognizes the value of further strengthening enterprise-wide coordination, prioritization and visibility of projects that span multiple areas or service lines, particularly initiatives with significant technology and transformation components. The Service notes that major technology and transformation initiatives are currently planned, governed and overseen using established project management practices, including documented business cases, budgeting assumptions and contingencies, governance checkpoints and Board-approved funding decisions. Information on these initiatives is provided to the Board through multiple established channels, including business cases, Board reports, capital budget

submissions and project-specific briefings.

The recommendation is understood as an opportunity to enhance the integration and consistency of project reporting and coordination and capital budget practices.

As part of the Service's broader operating and modernization frameworks already in development, an Enterprise Project Management Office (EPMO) capability will be advanced through the Strategy & Transformation pillar, under the direction of CTO Colin Stairs. This function will build on existing project management practices and will be designed to support a whole-of-TPS approach by:

- Providing enterprise-level coordination for cross-pillar and cross-service line initiatives;
- Supporting alignment between strategic priorities, operational planning and technology modernization; and
- Enabling better and more consistent project status reporting for executive leadership and the Board

This work is intended to complement the Service's established operational frameworks, including the Community Safety and Well-Being operational roadmap, the Service Line operating model and IM's Analytics Framework, which together support alignment, transparency and measurable progress.

ITS will need to continue to maintain an IT-specific project management function, to support ongoing initiatives already in flight. ITS PMO will ensure alignment with this new EPMO function to maintain consistency and coordination.

Implementation will be phased and aligned with the development of related operating plans, including the Service's Technology Plan, and broader transformation initiatives; current estimate is implementation by Q4 2028. The Board will be kept informed through regular reporting as this EPMO capability is further defined and operationalized.

Recommendation 4: The Board request the Chief of Police, Toronto Police Service, to develop a clear and easy to understand technology reporting package for the Board to be provided on a regular basis. The reporting package should include a consistent template or dashboard providing:

a. Status of progress on meeting timelines, budget and expected benefits on technology projects, including any revisions from the original budget and timelines

b. Baseline metrics to help measure benefits following introduction of new or enhanced systems

c. Challenges impacting the implementation and mitigation strategies for risks

d. An outlook, including longer-term, of planned major technology investments, including future upgrades, rationalizations, replacements, projects, and new technology initiatives.

Management Response: ☒ Agree ☐ Disagree
Comments/Action Plan/Time Frame: TPS agrees with this recommendation. While elements of technology reporting currently exist across project, portfolio, and financial management processes, reporting is not yet fully standardized, centralized, or consistently aligned to Board-level requirements. To address this, the Service is advancing a Delivery Performance capability within the ITS pillar. This function will be responsible for defining and maintaining a standardized technology reporting framework, and producing a consolidated reporting package for Executive and Board-level consumption. Key components will include: • Standardized reporting templates and dashboards covering schedule, budget, scope, risks and dependencies across major technology initiatives; • Benefits realization tracking, including development of baseline metrics and post-implementation measurement; • Integrated risk and issue reporting, including mitigation strategies and escalation mechanisms; • Forward-looking investment visibility, aligned to the forthcoming technology roadmap, including planned upgrades, replacements and new initiatives. This work will be aligned with broader corporate initiatives currently in progress, including the ERM framework and the EPMO program. As these functions mature, they are expected to assume responsibility for consolidated reporting to the Board, establishing a consistent, enterprise-wide approach. In the interim, Delivery Performance will support IT-specific reporting, ensuring outputs are decision-oriented, aligned to governance expectations, and operationally sustainable. While the initial design and piloting of reporting templates is expected to begin in 2026, full implementation will require alignment and resource prioritization through the 2027 planning and budget cycle. Alignment with ERM and EPMO will follow timelines for those respective initiatives (current estimate is implementation by Q4 2028).

Recommendation 5: The Auditor General recommends that the Board ensures its Strategic Plan provides governance direction for the Toronto Police Service to develop and implement a Technology Plan and an Enterprise Risk Management framework, to hold the Chief and the TPS accountable for achieving its technology objectives and outlining the reporting on technology matters required by the Board.

Management Response: ☒ Agree ☐ Disagree
Comments/Action Plan/Time Frame: **Board response:** The Toronto Police Service Board will ensure that its Strategic Plan provides governance direction for the Toronto Police Service to develop and implement a Technology Plan and an Enterprise Risk Management (ERM) Framework.

The Board will establish an Audit & Risk Management Committee to provide structured oversight of enterprise risk management, internal audit, and strategic plan implementation. This will include oversight of the Toronto Police Service's development and implementation of a Technology Plan and ERM Framework.

The Strategic Plan is expected to be considered by the Board at its May 2026 meeting, aligned with its consideration of this audit report and the establishment of the Audit & Risk Management Committee.

Management comment:
TPS agrees with this recommendation.

The Service will work to support the Board in fulfilling this recommendation.

Recommendation 6: The Board request the Chief of Police, Toronto Police Service, to strengthen its Technology Strategy to include:

a. Key performance indicators in relation to IT benefits framework

b. Approach to technology risk treatment

c. A process to assess the organization's alignment between the Toronto Police Service Board's Strategic Plan and the objectives set by the Toronto Police Service to deliver technology.

Management Response: ☒ Agree ☐ Disagree
Comments/Action Plan/Time Frame: TPS agrees with this recommendation. This work will be advanced through the Service's Technology Plan and aligned with the Board's Strategic Plan. The Service will ensure performance indicators, risk treatment and alignment processes are integrated into existing planning and reporting cycles. Early timeline expectations will be formulated once planning is underway; current estimate is implementation by Q4 2028.

Recommendation 7: The Board request the Chief of Police, Toronto Police Service, to implement a process for managing the review and update of technology policies, to include:

a. Creating an index for IT policies and procedures

b. Ensuring that all technology policies have clearly assigned owners and review frequency timelines

c. Performing a regular review to update policies according to their established timelines.

Management Response: ☒ Agree ☐ Disagree
Comments/Action Plan/Time Frame: TPS agrees with this recommendation in principle. Implementation is dependent upon obtaining

appropriate budget and resource allocations to support.

The Service acknowledges the importance of maintaining current, clearly-owned and consistently-reviewed technology policies to support effective governance, risk management, cybersecurity, and the delivery of modern policing services. A structured approach to technology policy management aligns with the Board's forthcoming Strategic Plan priority of Transparent and Trusted Governance, including expectations for accountability, evidence-based decision-making, and the proactive identification and mitigation of enterprise risks.

The Service notes that, while some ITS unit-specific policies have not been updated for a number of years, updates are undertaken as required, within existing resource constraints. The AG's observations primarily relate to ITS unit-specific policies rather than Service-wide governance instruments, which are managed through established Service-level policy frameworks.

While the Service agrees with the intent of this recommendation, establishing a sustainable technology policy review and maintenance process will require additional dedicated capacity with the ITS pillar. Current resourcing levels are insufficient to support ongoing policy inventory management, coordination, review, update and governance oversight activities. Based on comparable functions, an additional 2-3 full-time equivalents may be required to operationalize and sustain this capability.

This process can be operationalized through the introduction of a Delivery Performance function within ITS, contingent on the allocation of appropriate funding.

As part of the Service's broader Technology Plan and ERM framework, options to advance this recommendation will be assessed, including phased implementation, prioritization of higher-risk policy areas, and consideration of future resource requirements through established planning and budget processes (current estimate is implementation by Q4 2028). Progress and constraints will be communicated through established reporting mechanisms, to ensure transparency and alignment with Command and Board expectations.

Recommendation 8: The Board request the Chief of Police, Toronto Police Service, to strengthen its Project Management Framework to ensure:

a. Privacy impact assessments are performed for all technology projects including new technologies involving personal data

b. Results of privacy impact assessments are recorded and tracked for addressing risks

c. Where privacy risks categorized as high or medium are not fully mitigated before the system's go-live date, a formal risk acceptance describing compensating controls should be signed by the risk and project owners, including the Chief Information Security Officer, the Chief Transformation Officer, and, where appropriate based on the level of risk being accepted, the Chief of Police

d. The privacy risks which are categorized as high and not fully mitigated are reported to the Board and executive leadership.

Management Response: ☒ Agree ☐ Disagree
Comments/Action Plan/Time Frame: TPS agrees with this recommendation. Privacy Impact Assessments (PIA) are an important aspect of overall Information Management Assessments. PIAs are currently conducted for projects that involve personal information. The results of the PIA are recorded in the PIA itself, introducing a more modern risk/recommendation tracker would improve the timeliness of follow-ups. Staffing implications will need to be assessed where that scope is broadened, or evergreen assessments are conducted beyond current state. Risks identified in PIAs are either remediated or their risk accepted before a solution goes live. However, this process will be reviewed to improve the recording of risk ownership, risk treatment, and risks status over time. These form part of current IM Issues logs and can support broader ERM efforts. Further, IM will review opportunities to improve senior management oversight on risks with a significant residual rating, in line with the aforementioned ERM framework and EPMO program. Enhancement to tracking and oversight will require both process refinement and assessment of supporting tools and resourcing. Current estimate is implementation by Q4 2028.

Recommendation 9: The Board request the Chief of Police, Toronto Police Service, to strengthen data governance and privacy by implementing a process to:

a. Perform periodic reviews of user access profiles with respect to assigned roles and the required level of access to data and IT systems

b. Deactivate user access where such access is not needed

c. Obtain annual attestation from all TPS members and contractors, to remind them of their obligations under their Oath or Affirmation of Office, to comply with policies related to accessing and maintaining required privacy of confidential data and systems.

Management Response: ☒ Agree ☐ Disagree
Comments/Action Plan/Time Frame: TPS agrees with this recommendation. Implementation is dependent upon obtaining appropriate budget and resource allocations to support. This recommendation will be incorporated into the Service's Anti-Corruption initiative, to ensure alignment and avoid duplicate governance structures. In order to successfully implement this recommendation as specifically outlined, additional funding and resources will be required to support: • Staffing to proactively review and perform remediation activities • Change in access control technology (multi-year IT project and investment) Attestation for all TPS members at time of sign-on is already in place. IM is currently working with

the Toronto Police College on enhanced training initiatives. Extended use of auditing system capabilities is part of the 2026/2027 IM roadmaps for the Information Privacy & Access and Data Management units.

Through the Anti-Corruption initiative, the Service will work towards a strengthened process for user access that is operationally feasible.

Recommendation 10: The Board request the Chief of Police, Toronto Police Service, to:

a. Take a dedicated approach to data governance which establishes data owners, stewards, and custodians to oversee data quality and security, to address the areas for improvement identified in this report

b. Develop and provide training for members to ensure they understand their responsibilities for securing data under their control and maintaining the required privacy for it.

Management Response: ☒ Agree ☐ Disagree

Comments/Action Plan/Time Frame:

TPS agrees with this recommendation.

The Data Management Unit has been recently formed, with a mandate to support enhanced data governance, and enable data owners, stewards, and custodians across the Service. This work is in the Data Management Unit 2026/2027 roadmaps and is supported by the Information Privacy & Access Unit.

Canadian Police Knowledge Network training related to general privacy and security topics was previously developed and implemented by IM teams. IM will review its contents to determine if separate training is required for the different data governance roles.

Recommendation 11: The Board request the Chief of Police, Toronto Police Service, to review the current mandate and resources assigned to the Chief Information Security Officer; the review should include:

a. Independence of the role of the Chief Information Security Officer with respect to organizational reporting structure

b. Adequacy of resources to develop and implement cybersecurity policies across the Toronto Police Service

c. Direct access to the necessary cybersecurity information and reports generated across the organization

d. Mandatory involvement in projects and initiatives that require a cybersecurity perspective

e. Providing regular reports to executive leadership and the Board on the status of cybersecurity risks across the organization

f. Taking ownership of cybersecurity training and education such as, social engineering awareness training and phishing tests.

Management Response: ☒ Agree ☐ Disagree
Comments/Action Plan/Time Frame: TPS agrees with this recommendation. The Service recognizes cybersecurity as a critical risk that underpins service continuity, public trust, protection of sensitive information and the effective delivery of modern policing services. Reviewing the mandate of the Chief Information Security Officer (CISO) aligns with the Board's forthcoming Strategic Priority of Transparent and Trusted Governance, the Service's commitment to proactive ERM (outlined in management response to recommendation #2), and the role of technology modernization as an enabler of accountable and consistent service delivery. The Service notes that some foundational elements of the activities outlined for review in this recommendation are already taking place, including CISO having direct access to cybersecurity reports and information generated by IM units, and CISO leadership in training and education awareness campaigns. As recommended, the Service will review the current mandate, reporting structure, and resources assigned to CISO to ensure the role continues to be effective as the Service's technology environment evolves. The review will be informed by the Service's broader Technology Plan, Enterprise Risk Management framework, Anti-Corruption initiative, and other modernization initiatives. IM will be engaged and collaborate as part of this recommendation's efforts and ensuring an overall RACI matrix covers aspects of work in this space. The Service will consider options to strengthen capacity beyond the current single-incumbent model. Where gaps are identified, the Service will identify resource, governance and structural changes required to support a sustainable and enterprise-wide cybersecurity function. Current estimate is completion by Q4 2028.

Recommendation 12: The Board request the Chief of Police, Toronto Police Service, to establish a process to review vendors' cybersecurity attestation reports regularly to determine whether:

a. Vendors' services remain certified or attested under industry recognized standards

b. Cybersecurity weaknesses identified in the attestation reports are addressed by the vendors, where possible

c. Where weaknesses identified in the attestation reports have not been addressed by the vendors, to validate that risks to the TPS data and systems are assessed, and that non-compliance is addressed according to contractual obligations.

Management Response: ☒ Agree ☐ Disagree
Comments/Action Plan/Time Frame: The Service agrees with the recommendation. The Service currently maintains a process to obtain vendor cybersecurity attestations as part of vendor due diligence and ongoing vendor management. These activities are conducted in accordance with industry-recognized practices for public sector and enterprise consumers of third party or Software-as-a-Service (SaaS) platforms. Attestation reports are reviewed to confirm certification status and to identify material risks relevant to the Service's use of those services. This review activity is coordinated through established accountabilities within the Service's information security and risk management functions. TPS will undertake to annually analyze vendor relationships and attestations to determine where gaps may exist and to feed these upwards into an enterprise risk management process to be managed as part of Third Party Cyber risk. • Establishing a centralized function to perform ongoing, detailed analysis and tracking of all vendor attestation findings would require significant specialized resources and would not be proportionate to the Service's contractual authority or risk exposure as a consumer of services; • Vendor-specific non-compliance actions are constrained by contractual mechanisms and service-level agreements, which vary significantly by vendor and cannot be uniformly enforced through a centralized Service-led process. The Service will: • Obtain and retain vendor cybersecurity attestations on a regular basis; • Review reports at an appropriate, risk-based level to confirm certification status and identify material risks; • Assess identified risks to Service data and systems in alignment with the Service's broader risk management practices; and • Address vendor-related cybersecurity risks through established contractual and vendor governance mechanisms, including escalations where risks exceed acceptable tolerance.

Recommendation 13: The Board request the Chief of Police, Toronto Police Service, to review existing hiring practices, particularly for IT positions, to:

a. Develop and formalize criteria for reporting on long outstanding vacancies, reasons for delays, and their impact on operations

b. Identify tasks and processes that hinder filling of vacancies in a timely manner

c. Review hiring lead times, target turnover and vacancy levels, and revise processes where needed to address delays in completing the hiring of IT positions in a timely manner

d. Identify IT positions of highest risk to be prioritized and resourced in selecting vacancies to be filled.

Management Response: ☒ Agree ☐ Disagree
Comments/Action Plan/Time Frame: TPS agrees with this recommendation. One of the priorities that will be outlined in the Board's forthcoming Strategic Plan is supporting an agile and engaged workforce. To support this priority, the Service will plan, develop and design measures to support continuity, service effectiveness and resilience. The Service is developing a comprehensive People Plan addressing recruitment, retention, training and development, succession planning, career pathways, promotion processes and workforce wellbeing over a multi-year horizon. Within this plan, the Service will also focus on work to enhance internal mobility across commands, functions and roles so that talent can be developed and deployed in ways that better support both operational needs and member growth. Reviewing practices to better fill vacant technology-related positions will be an important component of this plan. Current estimate is implementation by 2029.

Recommendation 14: The Board request the Chief of Police, Toronto Police Service, to:

a. Explore the feasibility of implementing technical controls to monitor, control, or block access to unauthorized AI tools where needed

b. Ensure that the mandatory training, including ongoing refreshers, on responsible use of AI tools is rolled out for all Toronto Police Service members.

Management Response: ☒ Agree ☐ Disagree
Comments/Action Plan/Time Frame: TPS agrees with this recommendation in principle. Implementation is dependent upon obtaining appropriate budget and resource allocations to support. The Service is exploring the feasibility of using existing tools to monitor, control or block access to unauthorized AI tools; however, this work is limited in scope. Fully preventing or controlling the use of internet-based AI tools through technical controls alone is not realistic. Any expansion beyond the current limited feasibility assessment will require careful prioritization, additional resources and a combination of technical controls, policy measures and training rather than technical solutions alone. As part of the Service's broader Technology Plan and Enterprise Risk Management framework, the Service will assess options to advance this recommendation, including consideration of future resource requirements to support implementing required technical controls and training protocols, through established planning and budget processes (current estimate is implementation by Q4 2028).

Recommendation 15: The Auditor General recommends that:

a. The Board ensure a process is implemented to update Board policies in a timely manner

b. The Board update the AI Policy to include consideration of non-policing uses of AI in addition to policing uses, and that the policy be subject to a shorter review cycle.

Management Response: ☒ Agree ☐ Disagree
Comments/Action Plan/Time Frame: **Board response:** As part of the Board's regular policy review process, the Board will conduct a review of the AI Policy by Q4 2027, including consideration of both policing and non-policing uses of AI. **Management comment:** TPS agrees with this recommendation. The Service will work to support the Board in fulfilling this recommendation.

AUDITOR GENERAL TORONTO