

Audit of the Toronto Police Service's Information Technology Governance: Driving Improved Accountability and Transparency in Achieving Technology Objectives

Date: May 4, 2026

To: Toronto Police Service Board

From: Auditor General

Wards: All

SUMMARY

The Toronto Police Service (TPS) is Canada's largest municipal police force. It has 8,200 members, who make extensive use of Information Technology (IT) to deliver key policing activities.

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

This report includes a total of 15 recommendations, with 13 recommendations to the TPS and two recommendations to the Toronto Police Service Board (TPSB, or the Board). The recommendations for improvement are in three key areas:

- A. Improving the IT Governance Framework: including an Enterprise Risk Management function, providing consistent and holistic reporting on technology projects to the Board, strengthening the TPS's technology strategy, and updating technology related policies and procedures
- B. Strengthening Data Governance, Privacy and Information Security: ensuring confidential and sensitive data is well managed and controlled
- C. Improvement over Operational IT Functions: ensuring sufficient resourcing to achieve technology objectives, including filling IT vacancies in a timely manner, and training on artificial intelligence tools

RECOMMENDATIONS

The Auditor General recommends the following:

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.
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.
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.
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.

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.
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.
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.

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.

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.

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.

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.

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.

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.

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.

FINANCIAL IMPACT

By addressing the recommendations in this report, it will help the TPS and TPSB to further mature and strengthen their approach to IT governance. It will improve the TPS's monitoring and reporting of technology related risks, as well as reporting to the Board on planned and in-progress technology projects and initiatives. This will better inform decision making on technology matters, including resourcing required to achieve technology objectives, and will also help the TPS fully realize the intended benefits of its technology projects. It will also further strengthen TPS's IT controls, including data governance and privacy. The resulting costs and financial implications of any anticipated efficiencies, savings, and cost avoidance could not be determined at the time of this report.

DECISION HISTORY

The Auditor General's 2025 Audit Work Plan included an audit of the Toronto Police Service's IT Governance. The Auditor General's 2025 Work Plan is available at:

<https://www.toronto.ca/legdocs/mmis/2024/au/bgrd/backgroundfile-250975.pdf>

COMMENTS

A high-level summary of key audit findings is provided in the Audit at a Glance.

Towards the end of our audit, the TPSB passed a motion at its March 4, 2026 Board meeting¹ asking that our audit report highlight matters related to data governance and privacy in this report, which may inform the Board's oversight in light of Project South.² Data governance and privacy were already included in the scope of this audit at a high level, and recommendations 8 through 12 in the report directly relate to this subject matter. The remaining 10 recommendations relating to strengthening IT governance, enterprise risk management, and reporting on technology projects will also complement improving the TPS's approach to handling data and privacy more effectively.

The attached audit report, Attachment 1, provides the TPSB with the detailed audit results and recommendations, together with the TPS's management and Board response in Appendix 1.

TPS management and the TPSB have agreed to all 15 recommendations, which will help further mature and strengthen the TPSB's technology oversight, and the TPS's approach to IT Governance. The Auditor General will follow-up on the implementation of these recommendations and will report back to the Board on the status of implementation at a later date after management completes the implementation.

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.](#)

CONTACT

Syed Ali, Assistant Auditor General, Auditor General's Office
Tel: (416) 392-8438, E-mail: Syed.Ali@toronto.ca

Andrew Krupowicz, Senior Audit Manager, Auditor General's Office
Tel: (416) 392-3703, E-mail: Andrew.Krupowicz@toronto.ca

SIGNATURE



Tara Anderson
Auditor General

ATTACHMENTS

Attachment 1: Audit of the Toronto Police Service's Information Technology Governance: Driving improved accountability and transparency in achieving technology objectives