City of Saskatoon

CYBERSECURITY MATURITY ASSESSMENT & CONTROLS AUDIT

Terms of Reference

Independent Office of the City Auditor

August 6, 2025

TERMS OF REFERENCE

Background

The Internal Audit Foundation's *Risk in Focus 2025*[1] report found that Cybersecurity is the top risk facing organizations globally and it is expected to remain that way for the next three years.

The Canadian Centre for Cyber Security's *National Cyber Threat Assessment 2025-2026*[2] indicates that cybercrime remains a persistent, widespread, and disruptive threat and is becoming more complex and sophisticated, including the use of artificial intelligence. Further, the report notes that foreign state-sponsored cyber threat actors are becoming more aggressive, including attempting to deny service, delete or leak data, manipulate industrial control systems, and targeting critical civilian infrastructure.

Cybersecurity remains a critical concern for the City of Saskatoon (City) as it:

- Manages critical services such as water supply, power distribution, and transportation, which, if disrupted, could negatively impact public safety and wellbeing.
- Holds a significant amount of sensitive personal and financial data on its residents, which, if compromised, could result in privacy breaches and/or financial losses.

In accordance with the approved 2025-2026 Audit Plan, the Independent Office of the City Auditor (Office) has initiated the audit of the City's Cybersecurity Program (Program).

Objective

The engagement includes two components, the objective of each is listed below:

1. **Cybersecurity Maturity Assessment:** Assess the maturity of the City's current cybersecurity program against the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) Version 2.0.
2. **Cybersecurity Controls Audit:** Assess the effectiveness of the City's key controls to prevent and/or detect cybersecurity threats.

---

[1] *Global Summary: Risk in Focus 2025 – Hot Topics for Internal Auditors.* Internal Audit Foundation, 2024. https://www.theiia.org/globalassets/site/foundation/latest-research-and-products/risk-in-focus/2025/global-summary-risk-in-focus-2025-hot-topics.pdf.

[2] *National Cyber Threat Assessment 2025–2026.* Canadian Centre for Cyber Security, 2024. https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf.

Scope

The scope of the engagement includes:

- A review of the current state of the Program including policies, processes, and other relevant documentations available at the time of the assessment.
- Both the Information Technology (IT) and Operational Technology (OT) environments.
- The following relevant compliance obligations: *The Local Authority Freedom of Information and Protection of Privacy Act* (LAFOIP), *The Health Information Protection Act* (HIPA), and the Payment Card Industry Data Security Standard (PCI-DSS).

The Cybersecurity Maturity Assessment includes the six core NIST CSF 2.0 functions (Govern, Identify, Protect, Detect, Respond, and Recover) and all applicable subcategories.

The Cybersecurity Controls Audit includes the following key controls:

- Multi-Factor Authentication (MFA) for remote access and privileged accounts
- Endpoint Detection and Response (EDR) solutions
- Secured, encrypted, and regularly tested backup systems
- Email filtering and web security controls
- Patch management processes
- Cyber incident response planning and testing
- Cybersecurity awareness training and phishing simulation programs
- Network security logging and monitoring capabilities

The scope does not include activities related to the independent boards and corporations.

Approach

The Office collaborated with the Administration (i.e., Cybersecurity Lead and Supply Chain) to engage an external service provider to deliver both components of this engagement.

The Administration had a Cybersecurity Maturity Assessment performed in 2023 and had budgeted for an updated assessment in 2025. Although this portion of the engagement is being led by an external service provider and funded by the IT budget, the Office will be involved in the relevant meetings to ensure ability to rely on the work performed. The Maturity Assessment will be performed through interviews and a relevant documentation review but will not include detailed testing or validation.

The Cybersecurity Controls Audit will be performed by the external service provider, under the direction, control and budget of the Office, and will include appropriate test of controls.

Deliverables

The audit report will include the results of the Cybersecurity Maturity Assessment and Controls Audit highlighting strengths of the Program along with recommendations related to potential areas of improvement. The draft audit report will be presented to Administration for review and comment prior to finalization. The final audit report will be presented In-Camera to the Standing Policy Committee on Finance and is expected to be complete in Q4 2025.