Subject: Office of the Auditor General (OAG) - Follow-up Report – Cybersecurity Audit

File Number: ACS2025-OAG-BVG-012

Report to Audit Committee on 12 September 2025

and Council 24 September 2025

Submitted on September 10, 2025 by Nathalie Gougeon, Auditor General

Contact Person: Nathalie Gougeon, Auditor General, Office of the Auditor General (OAG)

613-580-9602: oag@ottawa.ca

Ward: Citywide

Objet : Bureau de la vérificatrice générale (BVG) – Rapport de suivi : Vérification de la cybersécurité

Numéro de dossier : ACS2025-OAG-BVG-012

Rapport présenté au Comité de la vérification

Rapport soumis le 12 septembre 2025

et au Conseil le 24 septembre 2025

Soumis le 2025-09-10 par Nathalie Gougeon, Vérificatrice générale

Personne ressource : Nathalie Gougeon, Vérificatrice générale, Bureau de la Vérificatrice générale (BVG)

613-580-9602: bvg@ottawa.ca

Quartier : À l'échelle de la ville

REPORT RECOMMENDATION(S)

That the Audit Committee receive the follow-up report and recommend that Council consider and approve the recommendations.

RECOMMANDATION(S) DU RAPPORT

Que le Comité de la vérification reçoive le rapport de suivi et recommande au Conseil d'examiner les recommandations, à des fins d'approbation.

BACKGROUND

In January 2023, the Office of the Auditor General (OAG) commenced an Audit of Cybersecurity which had been included as part of the 2022-2023 work plan, approved by Council on December 8, 2021. A preliminary audit report was tabled, in-camera, at the end of the completion of the planning phase of the audit in September 2023. The audit continued through 2023, and a final audit report was presented, in-camera, to the Audit Committee in November 2023.

As per the OAG Audit Charter, a standard follow-up process is required to be performed, whereby the OAG performs an inquiry of management to confirm the steps taken to implement the recommendations and may perform further tests.

DISCUSSION

The OAG is providing a report to the Audit Committee on the results of follow up procedures performed related to the Audit of Cybersecurity.

Details can be found in the Follow-up Report – Cybersecurity Audit (**Document 1).**

FINANCIAL IMPLICATIONS

There are no financial implications associated with this report.

LEGAL IMPLICATIONS

There are no legal impediments to the Audit Committee and Council considering this report. However, the City Clerk and City Solicitor, in consultation with the Auditor General, have recommended that the Follow-up Report – Cybersecurity Audit be presented to the Committee in closed session and not reported out. The comments set out below explain the underlying rationale for this recommended approach as it relates to the "security of the property" of the City, which is a statutory exemption for a closed meeting.

Subsection 239(2)(a) of the Municipal Act, 2001 stipulates that a meeting or part of a meeting may be closed to the public if the subject matter being considered is “the security of the property of the municipality or local board” and this and other exemptions are reiterated in Section 13 of the City’s Procedure By-law.

The Follow-up Report – Cybersecurity Audit communicates the results of the OAG’s follow-up work completed on the previously issued Audit of Cybersecurity. It discusses risks related to cybersecurity.

In order for a municipality to rely upon the “security of the property” exemption to hold a closed meeting, it must be able to establish that:

1. It owns the corporeal or incorporeal property identified; and

2. The consideration of the matter at the meeting is, in fact, the security of that property, including taking the appropriate measures to prevent the loss of, or damage to, that property.

The discretionary exception to the open meeting rule for the ‘security of the property’ would meet that two-part test and apply with regards to the Committee considering this report. The property of the City under consideration within the Follow-up Report – Cybersecurity Audit includes processes related to IT networks and systems supporting City operations.

COMMENTS BY THE WARD COUNCILLOR(S)

This is a city-wide issue.

CONSULTATION

As this is considered an internal administrative matter, no public consultation was undertaken.

ACCESSIBILITY IMPACTS

There are no accessibility impacts associated with this report.

RISK MANAGEMENT IMPLICATIONS

The principles of IT risk management underpin the findings and recommendations outlined within the Follow-up Report - Cybersecurity Audit.

TERM OF COUNCIL PRIORITIES

This report supports the Term of Council Priority related to Governance, Planning and Decision Making.

SUPPORTING DOCUMENTATION

Document 1 - OAG: Follow-up Report – Cybersecurity Audit (confidential, on file with the Office of the Auditor General)

Document 1 - BVG: Rapport de suivi : Vérification de la cybersécurité (confidential, on file with the Office of the Auditor General)

DISPOSITION

The Office of the Auditor General will proceed according to the direction of the Audit Committee and Council in considering this report.