City of Hamilton

Report for Consideration

To:	Chair and Members Audit, Finance and Administration Committee
Date:	April 16, 2026
Report No:	AUD21004(d)
Subject/Title:	Cyber Security Follow Up Audit, Phase 2: Incident Response and Insurance Review
Ward(s) Affected:	(City Wide)

Recommendations

a) That the Confidential Audit Report, attached as Appendix “A” to Report AUD21004(d), **BE RECEIVED** for information and **REMAIN CONFIDENTIAL**.

b) That the Confidential Audit Report, attached as Appendix “B” to Report AUD21004(d), **BE RECEIVED** for information and **REMAIN CONFIDENTIAL**.

c) That the management responses in Appendix “C” to Report AUD21004(d) **BE APPROVED** and **REMAIN CONFIDENTIAL**; and

d) That the Chief Information Officer (Acting) and the General Manager of Finance and Corporate Services **BE DIRECTED** to implement the management responses contained in Appendix “C” to Report AUD21004(d) and report back to the Audit,

Finance and Administration Committee by August 2026, on the nature and status of actions taken in response to the Audit Report.

Key Facts

- The Office of the Auditor General (OAG) is conducting a Cyber Security Follow Up Audit. This is the second in a series of four reports to be issued.
- The OAG's Cyber Security Audit was issued in April 2021.
- The topics of this report are Incident Response (an evaluation of City's incident response to the February 2024 breach) and Insurance Review (an assessment of the City's cyber insurance coverage at the time of the February 2024 breach).
- For both the incident response and insurance review, analysis OAG conducted found that there was significant room for improvement.
- The OAG has made 19 new recommendations to improve cyber and insurance practices.

Financial Considerations

Not applicable.

Background

On January 22, 2025, the OAG provided information in-camera about the planning phase of the Cyber Security Follow Up Audit to the Audit, Finance and Administration Committee (Report AUD21004(a)). On April 10, 2025, additional public reporting and disclosure was provided to the Audit, Finance and Administration Committee.

The original Cyber Security Audit was issued in April 2021 by the OAG. OAG was planning a follow-up audit in 2024 when the cybersecurity incident occurred, which caused delay and modification to the original scope of the review.

The Cyber Security Follow Up Audit consists of four parts, delivered in a series of reports. This is the second of four reports to be issued. Phase 1 (Report AUD21004(c) was presented at the October 2, 2025 Audit, Finance and Administration Committee meeting. The OAG received requests from Council to review the insurance coverage, so the OAG included this analysis as part of Phase 2 of the Follow Up Audit.

Cyber Security Follow Up Audit
Phase 1 – Pre-Breach Analysis Report Assessment of the City's cyber posture prior to the incident in February 2024, and progress made since the 2021 Audit, identifying root causes and systemic weaknesses for any gaps that remained at the time of the breach.
Phase 2 – Incident Handling Review and Insurance Review A. Evaluation of the incident response based on NIST SP 800-61, focusing on how effectively the incident was managed, including containment and immediate remediation measures. B. Assessment of insurance coverage at the time of the incident.
Phase 3 – Roadmap Assessment Review of the City of Hamilton's proposed cyber security roadmap to assess how well it addresses the gaps and issues identified in Phase 1 and OAG's 2021 Cyber Security Audit.
Phase 4 – Roadmap Financing Assessment Review to assess reasonability and overall soundness of the financing plan to fund the execution of the cyber security roadmap.

TODAY

Analysis

This report contains findings from Phase 2 of our Cyber Security Follow Up Audit. The focus of this review consists of A) an evaluation of the City's incident response and B) a

review of the City's insurance coverage at the time of the February 2024 ransomware attack.

The objectives Phase 2 were:

A. To assess the City of Hamilton's incident response to and management of the February 2024 ransomware attack against industry best practices, and to improve understanding of how the City's incident response can be improved in the future to assist the City's efforts in responding to any future cyber incidents.

B. To look at key events associated with the ransomware incident and the subsequent claim denial, and to examine whether City Council and staff members reasonably understood coverage limitations prior to the incident.

The key findings were:

Phase 2A

- Challenges were found across all stages of the City's incident response.
- At the time of the response, the City's practices, capabilities, and resources did not support an effective response.
- Gaps were found that hampered the City's ability to detect, respond to, and recover from the incident.

Phase 2B

- The ransomware incident and subsequent claim denial exposed gaps between cyber risk management, insurance procurement, and governance oversight.
- There was insufficient assurance prior to the incident that the cyber insurance policy would be applied as anticipated by the City.

- Governance processes did not adequately identify, escalate, or address the consequences of unmet underwriting conditions.
- This resulted in the existence of a significant uninsured financial impact.

Alternatives

Not applicable.

Relationship to Council Strategic Priorities

See 2022-2026 Council Priorities, Outcomes & Measures of Success | City of Hamilton for more information on Council's Priorities.

3. Responsiveness & Transparency
   3.3 Build a high performing public service
   3.4 Modernize City systems

Previous Reports Submitted

- Report AUD21004 Cyber Security Audit, April 22, 2021, Audit, Finance and Administration Committee meeting.
- Report AUD21004(a) Cyber Security Follow Up Audit – Planning Summary, January 16, 2025, Audit, Finance and Administration Committee meeting.
- Report AUD21004(b) Cyber Security Follow Up Audit – Additional Public Disclosure, April 10, 2025, Audit, Finance and Administration Committee meeting.
- Report AUD21004(c) Cyber Security Follow Up Audit, Phase 1: Pre-Breach Analysis Report, October 2, 2025, Audit Finance and Administration Committee meeting.

Consultation

Many interviews were conducted with City staff and management for this Follow Up Audit. These included the Interim Chief Information Officer, the Chief Information Security Officer, various staff and management in the Information Technology Division, the City Solicitor, Manager Risk Management Services, and several other relevant staff and management at the City of Hamilton.

The management response for Phase 2A Incident Response was provided by the Chief Information Officer (Acting) and the Chief Information Security Officer.

The management response for Phase 2B Insurance Review was provided by the City Solicitor and the Manager Risk Management Services.

Appendices and Schedules Attached

CONFIDENTIAL Appendix A: Cybersecurity Incident Response Assessment Report

Confidential Appendix A “Cybersecurity Incident Response Assessment Report” is private & confidential in accordance with Section 239(2)(a) of the Municipal Act 2001 as the subject matter pertains to the security of the property of the municipality or local board.

CONFIDENTIAL Appendix B: Cybersecurity Insurance Review Report

Confidential Appendix B “Cybersecurity Insurance Review Report” is private & confidential in accordance with Section 239(2)(e) of the Municipal Act 2001 as the subject matter pertains to litigation or potential litigation, including matters before administrative tribunals, affecting the municipality or local board.

CONFIDENTIAL Appendix C: Recommendations and Management Responses

Confidential Appendix C “Recommendations and Management Responses” is private & confidential in accordance with Section 239(2)(a) of the Municipal Act 2001 as the subject matter pertains to the security of the property of the municipality or local board.

Prepared by:

Brigitte Minard, Deputy Auditor General, Office of the Auditor General

Charles Brown, Auditor General, Office of the Auditor General

Valencia Risk, on behalf of the Office of the Auditor General

Submitted and Recommended by:

Charles Brown, Auditor General, Office of the Auditor General