

AUDITOR GENERAL

Halifax Regional Municipality



Follow-up Review – 2023 Audit: HRM IT: Management of Cybersecurity – Public

December 2025

December 4, 2025

This ***Follow-up Review – 2023 Audit: HRM IT: Management of Cybersecurity – Public***, completed under section 50(2) of the Halifax Regional Municipality Charter, is hereby submitted to the Audit and Finance Standing Committee of Regional Council.

Respectfully,

Original signed by

Andrew Atherton, CPA, CA
Auditor General
Halifax Regional Municipality

**AUDITOR
GENERAL**



Halifax Regional Municipality

Office of the Auditor General
Halifax Regional Municipality
33 Alderney Drive, Suite 620
Dartmouth, NS, B2Y 2N4
www.hrmauditorgeneral.ca
902.490.8407

Table of Contents

Overall Follow-up Results3

HRM IT: Management of Cybersecurity – Public – August 2023.....4

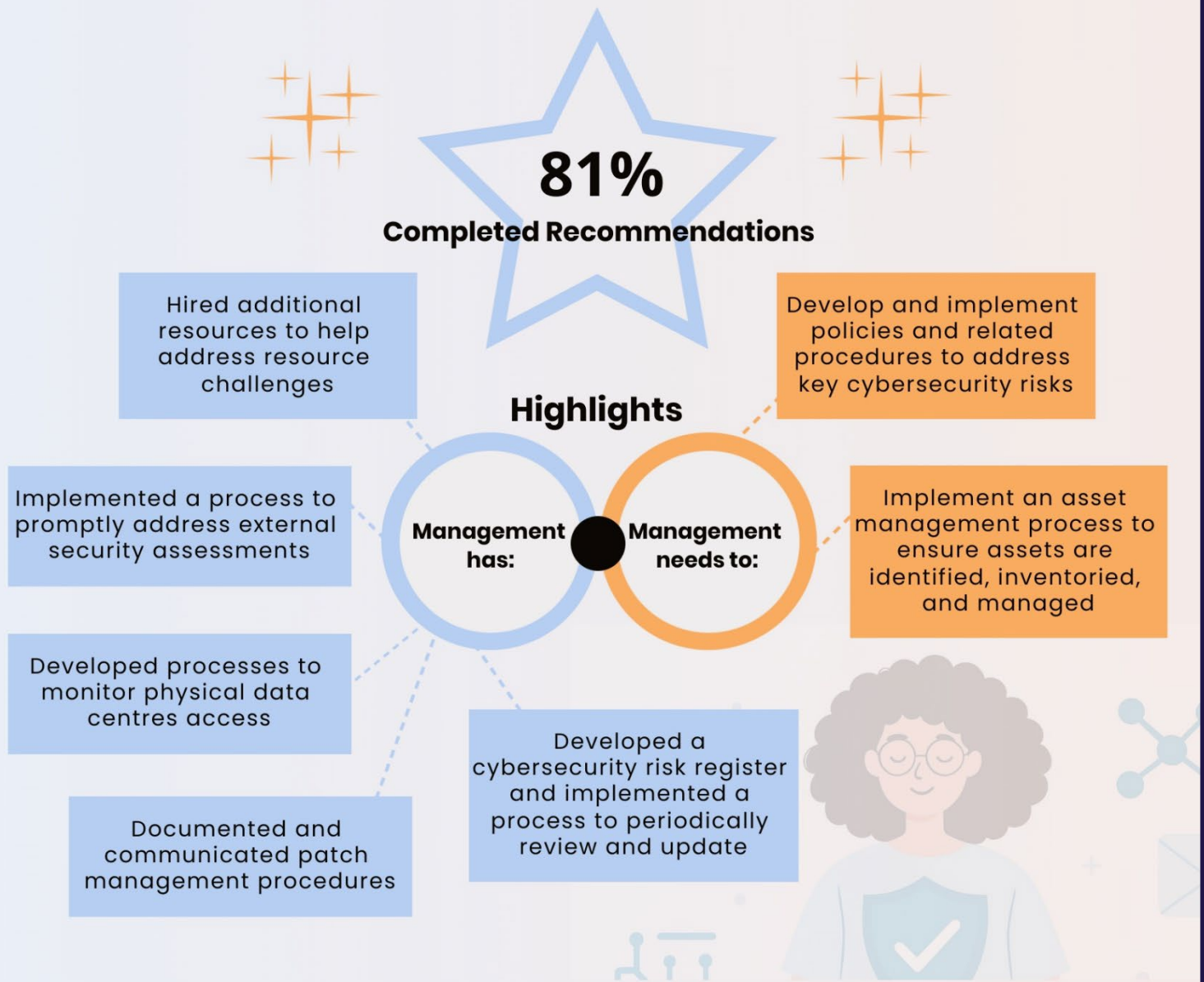
Background.....6

Objective and Scope6

Contact Information7

Follow-up Review – 2023 Audit:

HRM IT: Management of Cybersecurity – Public



Halifax Regional Municipality Auditor General
December 2025

HRM IT: Management of Cybersecurity – Public – August 2023

Implementation Status by Recommendation

| Recommendation | Business Unit | Status |
|---|------------------------|--------|
| 1. Information Technology management should assess resource needs to perform its cybersecurity duties and develop and implement plans to address the resource challenges. | Information Technology | ✓ |
| 2. Information Technology management should complete the cybersecurity risk register and implement a process to periodically review and update. | Information Technology | ✓ |
| 3. Information Technology management should implement a process to ensure recommendations from external security assessments in 2022 and 2023 are monitored and managed to ensure they are addressed in a timely manner. | Information Technology | ✓ |
| 4. Information Technology management should determine whether there are relevant recommendations from the 2018 threat risk assessment that are not covered by the 2023 assessment. Any remaining recommendations should be assessed and addressed if still valid. | Information Technology | ✓ |
| 5. Information Technology management should develop and implement policies and related procedures to address key cybersecurity risks. | Information Technology | ✗ |
| 6. Information Technology management should implement a process to receive and review vendor security submissions in a timely manner. Management should clearly assign responsibility for the process. | Information Technology | ✗ |
| 7. Information Technology management should replace physical locks at both datacentres immediately. | Information Technology | ✓ |
| 8. Information Technology management should implement a process to track keys and return to Corporate Security if no longer needed. | Information Technology | ✓ |

| Recommendation | Business Unit | Status |
|---|------------------------|--------|
| 9. Information Technology management should periodically review who has access to the datacentres and update as needed. | Information Technology | ✓ |
| 10. Information Technology management should implement a visitor log at all datacentre locations and require visitors be escorted by HRM IT management or staff. HRM employees and accessible through HRM communication channels. | Information Technology | ✓ |
| 11. Information Technology management should document and communicate patch management procedures | Information Technology | ✓ |
| 12. Information Technology management should determine and communicate an approved software list to IT staff who have the ability to download and install software. | Information Technology | ✓ |
| 13. Information Technology management should assess whether it is feasible to identify employees who access HRM systems but did not receive the training. If so, identified employees should be sent the training. | Information Technology | ✓ |
| 14. Information Technology management should provide HRM business units with a list of employees who have not completed the mandatory cybersecurity awareness training to allow business unit managers to follow up with staff. | Information Technology | ✓ |
| 15. Information Technology management should determine next steps for employees who repeatedly fail to identify simulated phishing emails. | Information Technology | ✓ |
| 16. Information Technology management should develop and implement an asset management process to ensure assets are identified, inventoried, and managed. | Information Technology | ✗ |

*Legend: ✓ = Completed ✗ = Incomplete

Background

The Office of the Auditor General, Halifax Regional Municipality, follows up audits previously reported by the office after 18 months. These follow-up reviews report the progress management had made implementing changes recommended by the Auditor General.

Objective and Scope

We completed a follow-up review of a report released in 2023.

- HRM IT: Management of Cybersecurity – Public

Our objective was to provide review level, or limited assurance, on HRM management's implementation of recommendations from this report. A limited assurance engagement provides a lower level of assurance than an audit. Conclusions are based on reasonability of what management tells us, and limited testing, rather than detailed testing, as would be found in an audit. This allows us to focus limited resources on new audits, while still providing assurance that management is addressing the issues we identified in past audits.

Our approach included discussing implementation with staff; reviewing policies, guidelines and processes; and other procedures we considered necessary.

This limited assurance engagement was conducted in accordance with the Canadian Standard on Assurance Engagements (CSAE) 3001 Direct Engagements published by the Chartered Professional Accountants of Canada.

We apply CPA Canada's Canadian Standard on Quality Management 1. Our staff comply with the independence and ethical requirements of the Chartered Professional Accountants of Nova Scotia Code of Conduct.

Contact Information

Office of the Auditor General
Halifax Regional Municipality
33 Alderney Drive, Suite 620
Dartmouth, NS, B2Y 2N4

Phone: 902.490.8407

Email: auditorgeneral@halifax.ca

Website: www.hrmauditorgeneral.ca

X: [@Halifax AG](#)