AUDITOR GENERAL

Halifax Regional Municipality

HRM IT: Management of Cybersecurity Audit – Public

August 2023

August 11, 2023

The following audit of **HRM IT: Management of Cybersecurity**, 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

Evangeline Colman-Sadd, 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

HRM IT: Management of Cybersecurity Audit

Not providing appropriate oversight to manage cybersecurity risks

Strategic plan identifies cybersecurity practices and risk management

- Lacks detailed plans with timelines
- Inadequate cybersecurity risk register

Management told us they have some resource concerns

- But have not assessed what resources are needed to address
- No request for additional resources in recent budget process

Policies and procedures need improvement

- Responsibilities for key processes not assigned
- Disagreements among management on who is responsible for some processes
- Patch management process documentation needs improvement
- Limited policies and procedures to manage network access

Good change management process

- Not always followed

Implemented cybersecurity awareness program

- Completion rates need improvement

Physical access needs to be further limited and better monitored

Auditor General Halifax Regional Municipality

August 2023

Public

Audit Results

Information Technology management is not providing appropriate oversight to manage cybersecurity risks. Management identifies cybersecurity risks but has limited policies and processes to document and manage them. In addition, responsibilities for processes in key areas, have not been determined.

The Information Technology business unit does not have adequate documented processes to support network cybersecurity. Management needs to develop policies that cover cybersecurity risk areas. Many processes were not documented, and, in some cases, there were disagreements among management on who was responsible for aspects of the process. The documented change management process reflects good practices. However, it is not always followed. Some physical controls were present but physical access to network infrastructure is not appropriately limited or monitored. Policies and procedures to manage access to the network need improvement. In 2022, management implemented a cybersecurity awareness training program that includes management, staff, and elected officials; however, completion rates need improvement.

This report contains some of our findings in these areas. There is also an in-camera report which provides more detail.

Oversight

Information Technology management is not providing appropriate oversight to ensure cybersecurity risks are managed. Information Technology's strategic plan includes cybersecurity practice review and risk management governance, but management lacks detailed plans and timelines to move forward with improvements. Management told us they have some resource concerns; however, they have not assessed the resources needed or requested additional resources. We noted the 2023-24 business plan does not assess current resources or identify additional resources needed to address strategic priorities.

Management identified cybersecurity risks through internal and external consultant reviews; however, these have not been effectively assessed and prioritized. HRM IT submitted some risks to the enterprise risk register and started a cybersecurity risk register but have not established timelines for completion. Management has not developed plans to address known issues. While certain cybersecurity roles and responsibilities are documented in management and staff job descriptions, there are key areas where it is not clear who is responsible. We also noted instances during the audit where management disagreed on which team was responsible for certain tasks.

Cybersecurity and risk management included as strategic areas but plans lacking

Information Technology's strategic plan includes cybersecurity practice review and security risk management governance. Management performed an internal assessment to review its cybersecurity practices and started a roadmap to address identified issues. The roadmap identifies high priority areas but has no detailed plans or timelines. Management told us they are unsure what resources they will need to implement the roadmap.

To address the security risk management governance objective, a cybersecurity risk register tied to enterprise risk management is needed. Management told us they had initial discussions with HRM's Risk and Insurance group but there are no plans or timelines for completion.

Cybersecurity resource concerns not sufficiently communicated

Information Technology management and staff expressed resourcing concerns throughout the audit. However, management has not assessed needs or requested additional resources.

Information Technology management briefed Regional Council on cybersecurity in 2022 and 2023. The 2023 briefing was provided in response to a councillor's request to understand what HRM is doing to prevent and prepare for cyber attacks. While it provided an overview of areas management has identified for focus, it did not specify that resource needs had not been identified or assessed. This matter is discussed in further detail in the in-camera report.

Cybersecurity roles and responsibilities not defined, clear, or understood

Although there are job descriptions for key management and staff roles with cybersecurity responsibilities, Information Technology has limited policies and procedures for key processes. Lack of clarity around who is responsible for key processes can lead to gaps. This area is discussed in more detail in the in-camera report.

Recommendation 1

Information Technology management should assess resource needs to perform its cybersecurity duties and develop and implement plans to address the resource challenges.

Management Response

Agreed. IT Management will work with the CAO to determine the maturity level the organization wishes to obtain in the Cybersecurity practice and its adherence to the NIST Cybersecurity Framework. From this, current resourcing will be assessed, and any required resource needs articulated.

Cybersecurity risks not appropriately managed

Control Area	Current State – HRM IT	Why It Matters/ Risk
Cybersecurity risk assessment	• Inadequate cybersecurity risk register • Management has a template • One risk evaluated • Three issues identified • No timelines for completion • Some cybersecurity risks identified but not captured centrally • External consultant prepared threat risk assessments • HRM IT prepared a control gap assessment	• Risk register should document and assess cybersecurity risks • Important to identify gaps and any mitigating controls • Risks that are not appropriately addressed could increase the impact and likelihood of an event impacting HRM's network. • Risk register helps inform management of cybersecurity risks. • Persistent gaps could allow hackers to penetrate HRM's network.
Critical system identification	• No exercise to identify the organization's critical systems • Some business applications categorized as critical • All systems given equal priority from a security perspective	• Important to identify systems that provide critical services or hold sensitive information to inform disaster recovery priorities. • Risk assessments help prioritize resources to protect these systems.

Control Area	Current State – HRM IT	Why It Matters/ Risk
Cybersecurity risk mitigation and response	• Management prepared a cybersecurity roadmap based on internal controls assessment. • However, no detailed plans and timelines to address • Management does not know what resources are needed	• Important to have plans and timelines to ensure cybersecurity risks are addressed in a timely manner
External security assessments	• Management had external consultants complete security assessments in 2018, 2022, and 2023 • Management needs to monitor consultant recommendations to ensure concerns are addressed.	• Security improvements strengthen the organization's security profile and help reduce the likelihood and impact of breaches and attacks.

Recommendation 2

Information Technology management should complete the cybersecurity risk register and implement a process to periodically review and update.

Management Response

Agreed. IT management will implement a process for periodic review and updates to the cybersecurity risk register.

Recommendation 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.

Management Response

Agreed. 2022/2023 recommendations have been captured in the Cyber audit record document. Plans for risk treatment actions will be developed and results captured as they are addressed.

Recommendation 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.

Management Response

Agreed. IT Management has reviewed the 2018 threat risk assessment and all unaddressed relevant recommendations are captured in the 2022 and 2023 assessments. These will be addressed through actions on those reports' recommendations.

Limited policies and procedures to address key cybersecurity risks

Control Area	Current State – HRM IT	Why It Matters/ Risk
Cybersecurity policies and procedures	• HRM IT has limited policies and procedures that cover cybersecurity risk areas, improvements are needed • Examples of areas for improvement include: • Access control management • Supply chain management • Configuration management	• If policies are not well communicated, processes may be inconsistent amongst staff. • Risks may not be appropriately managed.

Control Area	Current State – HRM IT	Why It Matters/ Risk
		• If policies are not regularly updated, they may no longer address existing security risks. • Procedures help to implement policies by ensuring process owners are defined, responsibilities are clear, and important steps in the process are understood.

Recommendation 5

Information Technology management should develop and implement policies and related procedures to address key cybersecurity risks.

Management Response

Agreed. Policies, procedures, and guidelines will be Included in the remediation actions, where applicable.

Vendor contract security requirements not monitored

Control Area	Current State – HRM IT	Why It Matters/ Risk
Cybersecurity contract management	• IT contracts included reasonable security terms and conditions • IT is not monitoring vendor submissions to ensure they comply with security requirements • Of five IT contracts we looked at, two required vendors to periodically submit security reports. We found:	• Important aspect of risk management, should be included in risk assessment and mitigation activities

Control Area	Current State – HRM IT	Why It Matters/ Risk
	• Vendors submitted reports; one vendor had incomplete submissions • Management did not review security reports. • Management of two IT teams do not agree on who is responsible for reviewing submissions • We did not find significant deficiencies in our review of the reports	• Outsourced services can impact availability, business continuity, and security over HRM's data • Contracts outline terms, such as security requirements, deliverables, and consequences if they are not met.

Recommendation 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.

Management Response

Agreed. Vendor submissions are received today. IT Management will implement a process to ensure they are appropriately reviewed.

Physical Access

HRM has physical security controls to access its datacentres which house critical network infrastructure. However, management and monitoring of access needs improvement. Policies and processes to manage swipe card and key access are informal. Datacentre access should be restricted and monitored. There were individuals with access to the datacentres that did not require it for their jobs. Unauthorized changes to critical network infrastructure could cause a breach of sensitive information or a loss of services, impacting HRM's ability to operate.

Physical controls to secure HRM datacentres and ensure availability

Control Area	Current State – HRM IT	Why It Matters/ Risk
Physical access controls	• There are physical access controls at HRM's datacentres to help restrict access to the network	• Restricts who can access critical IT infrastructure • Protects HRM's network from unauthorized access and physical damage
Visitor access records	• Visitor logs are kept for one of the two datacentres.	• Maintains a physical record of who had access to the facility • Allows supervisors to monitor visitor access to sensitive areas
Environmental controls	• Both datacentres had controls to regulate the environment and protect critical infrastructure: • Raised floors to protect equipment from floods • Air conditioning to prevent overheating • Fire suppression equipment • Smoke detectors	• Protects critical infrastructure from damage or failure to help ensure availability of HRM's IT systems

Control Area	Current State – HRM IT	Why It Matters/ Risk
Emergency power	• Both datacentres have emergency power supplies including: • Uninterrupted power supply • We observed in one datacentre • HRM Building Services confirmed it exists for entire building at other datacentre • Additionally, management told us the buildings where the datacentres are located have generators	• Allows for continued operations of HRM IT systems during a power failure.

Management of physical access needs improvement

Control Area	Current State – HRM IT	Why It Matters/ Risk
Physical access control policy	• No policies or procedures to manage physical access to datacentres	• Employees or vendors could be given access to critical infrastructure that they do not require for their job duties. • Could lead to unauthorized access to HRM's network
Third-party access procedure	• IT does not have documented procedures for visitors to access the datacentres • Example: requirement to escort visitors	• Visitors may pose a security threat to the organization. • Access should be managed to reduce the risk of introducing a threat or vulnerability to HRM systems.

Control Area	Current State – HRM IT	Why It Matters/ Risk
Physical access – swipe cards	• HRM's datacentres are secured through swipe card and key access. • We obtained swipe card access list and found employees with access who did not require it for their jobs. • Eleven of 23 employees with swipe card access to one datacentre did not require it. • Six of 18 employees with swipe card access to the other datacentre did not require it. • Management removed access when this was brought to their attention.	• Access to datacentres should be limited to staff who require it for their job. • Unauthorized access could lead to accidentally or intentionally: • Introducing vulnerabilities to HRM IT systems • Affecting the availability of HRM IT systems
Physical access – keys	• Each datacentre can be accessed by key, instead of using a swipe card. • Corporate Security's records indicate 12 keys are assigned to IT staff • IT management told us the keys were obtained from staff when swipe card access was introduced but were thrown out rather than returned to Corporate Security.	• Key access does not leave an audit trail the way swipe cards do. It is important keys are accurately tracked and secured. • Poor key management may give unauthorized individuals access to critical infrastructure which could lead to tampering with or breaching HRM's network.
Monitoring physical access	• No monitoring to confirm physical access to datacentres is limited	• Reviewing physical access records and logs can help detect suspicious activity or potential threats.

Recommendation 7

Information Technology management should replace physical locks at both datacentres immediately.

Management Response

Complete.

Recommendation 8

Information Technology management should implement a process to track keys and return to Corporate Security if no longer needed.

Management Response

Complete. Keys are controlled by Corporate Security, they have signed forms for the new keys for the DC's, only 3 are in existence.

Recommendation 9

Information Technology management should periodically review who has access to the datacentres and update as needed.

Management Response

Complete. Manager Enterprise Services & Infrastructure will request this report quarterly from Corporate Security until the ability to automate this report exists.

Recommendation 10

Information Technology management should implement a visitor log at all datacentre locations and require visitors be escorted by HRM IT management or staff.

Management Response

Complete. Visitor logs are now in place and visitors are required to sign in when escorted to either DC. Manager Enterprise Services & Infrastructure will review logs quarterly.

Network Access

No access management policies; some procedures

Control Area	Current State – HRM IT	Why It Matters/ Risk
Access management policies and procedures	• No documented access management policy; some documented procedures to manage user or administrator access to the corporate network	• Employees and third-party contractors/vendors could be given access to systems that they do not require as part of their job duties.

Recommendation 5 above addresses this issue.

System Protection

HRM IT needs to improve policies and documentation of its procedures to protect the network. There is a formal change management process. However, there is also a risk that changes are not identified and completed in a timely manner.

Change management process implemented; not always followed

Control Area	Current State – HRM IT	Why It Matters/ Risk
Change management	• IT has a documented process to manage changes to IT assets, including requirements to: ◦ Approve and document nonemergency changes prior to implementation ◦ Implement emergency changes and then document • We reviewed a sample of 60 change management tickets from the audit period:	• Clear processes and guidelines support consistent modification and updates to ensure the system is secure. • Change management process helps ensure review and approval to minimize the risk

Control Area	Current State – HRM IT	Why It Matters/ Risk
	- Changes were mostly documented, and approved as required - Changes for systems without test environments had rollback plans	of availability issues resulting from a change. - Important to limit the amount of changes that bypass this process to true emergencies

Limited patch management procedures

Control Area	Current State – HRM IT	Why It Matters/ Risk
Patch management	- For the areas we examined, HRM IT needs to improve documentation of its patch management processes.	- Important for staff to know who is responsible for identifying patches released by vendors to ensure potential security gaps addressed in timely manner - Clear process to outline how to assess risk of implementing patch and testing procedures help to limit potential system disruption

Recommendation 11

Information Technology management should document and communicate patch management procedures.

Management Response

Agreed. IT Management will document and communicate Polices, procedures and guidelines addressing vulnerability management for critical assets.

No approved software list

Control Area	Current State – HRM IT	Why It Matters/ Risk
Approved software list	• No list of approved software determined safe to install ◦ • Important to prevent installation of software that could harm the organization or is not supported ◦ • Management said they will publish an approved software list but there is no timeline for completion.	• If IT staff download unsafe or unsupported software, it could contain viruses and malware that could affect HRM's systems. • Only approved software that has been determined safe and has a process to ensure it is kept secure, should be allowed on HRM assets that connect to the network.

Recommendation 12

Information Technology management should determine and communicate an approved software list to IT staff who have the ability to download and install software.

Management Response

Agreed. IT Management will develop a process for determining approved software and create procedures and guidelines where appropriate.

Cybersecurity training and awareness program; some improvements needed

Control Area	Current State – HRM IT	Why It Matters/ Risk
Cybersecurity awareness training	• HRM IT rolled out an organization-wide cybersecurity awareness training program in October 2022. • Management told us training will be sent annually. • Employees given 30 days to complete • Thirty-one percent of employees assigned initial training in October 2022 had not completed it by mid-February 2023 • IT has not passed on the names of these employees to their respective business units for follow up • Eleven of 17 elected officials had not completed the training as of mid-February 2023 • Training sent to employees with HRM email addresses • We selected 30 employees and found three were not sent training • Management told us all eligible employees may not have received the training due to data issues • Training system sends ongoing simulated phishing emails	• Important for those with access to HRM systems to be aware of their role in protecting them from security risks. • Ongoing phishing simulations a good practice to reinforce training • Hackers target employees to manipulate them into performing actions or providing confidential information to try and gain access to the network. • Employees play an important role in detecting and

Control Area	Current State – HRM IT	Why It Matters/ Risk
	• Training automatically generates when employee clicks a simulated phish email • No process to monitor for employees who repeatedly click on simulated phishing links	preventing cybersecurity threats.

Recommendation 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.

Management Response

Agreed. IT Management will audit gaps in the assignment of training.

Recommendation 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.

Management Response

Agreed. IT Management will audit the compliance reporting function available within the tool and will inform business units regarding employees who have not completed the training with requirements to have the training completed.

Recommendation 15

Information Technology management should determine next steps for employees who repeatedly fail to identify simulated phishing emails.

Management Response

Agreed. IT Management will audit the phishing reporting function available within the tool and provide appropriate feedback to employees who repeatedly fail to identify simulated phishing emails.

System Availability

HRM IT needs to improve its processes to ensure HRM's network remains available. While there are documented backup procedures, improvements are needed. There is no asset management policy. There is an asset management procedure for some assets. We also found HRM does not have an accurate inventory of IT assets.

Processes to ensure system availability need improvement

Control Area	Current State – HRM IT	Why It Matters/ Risk
System backup procedure	• Some procedures for restoring from backup; improvements needed	• Backups allow for timely recovery of HRM systems and reduce the loss of data.
Asset management policy	• No asset management policy • There is a procedure for some assets	• Helps ensure assets are identified and accurately tracked by assigning asset owners and providing clear procedures

Control Area	Current State – HRM IT	Why It Matters/ Risk
Asset inventory list	• HRM, IT does not have an accurate inventory list of IT assets • Server inventory not up-to-date • Spreadsheet updated and provided during audit • Network device inventory not complete • Did not include spare items not in use • Computer inventory tracked in tool; list not accurate • Found computers not on the list • HRM IT does not know the location of 451 computers on its list • Management told us they are working on implementing additional features in its configuration management database that will act as a centralized asset management tool. • No timeline for when this will be completed	• Provides management with visibility into what assets exist and need to be managed and protected • An accurate asset inventory helps prevent and detect loss of assets and outstanding maintenance

Recommendation 16

Information Technology management should develop and implement an asset management process to ensure assets are identified, inventoried, and managed.

Management Response

Agreed. IT Management will review the asset management process for gaps and augment processes where required.

Background

HRM's Information Technology business unit is responsible for supporting Regional Council, and HRM management and staff, by providing customer service and technological expertise. IT is responsible for supporting business units in various areas such as:

- Access to devices and services
- Data analysis
- Business systems
- Cybersecurity
- Internal planning for disaster recovery

Within IT, cybersecurity is responsible for managing risks around technology, including:

- Ensuring the organization's security awareness program is up to date
- Regular monitoring and remediation of threats and cyber attacks
- Cybersecurity incident management and incident response planning

There is also an Architecture and Infrastructure team which helps ensure the technology infrastructure can support municipal services. This team is responsible for physical and cloud-based infrastructure such as datacentres, hardware, and networking devices.

The Service Management and Operations team is responsible to maintain and support business applications. The team is also responsible for providing personal devices, telecommunication services, and technical support.

About the Audit

We completed a performance audit of HRM IT Management of Cybersecurity. The purpose of the audit was to determine whether HRM appropriately manages cybersecurity risks to its network. Our role is to express an independent audit opinion of this area. The audit scope did not include Halifax Regional Police information technology systems. This area was audited in our 2021 Halifax Regional Police Information Technology Audit.

The objective of this audit was to assess whether Information Technology management provides appropriate oversight to manage cybersecurity risks and has adequate processes to support network cybersecurity.

We developed criteria for the audit. These were discussed with, and accepted as appropriate by, Information Technology management.

- Information Technology should maintain and use policies, procedures, and processes to identify, document, and manage cybersecurity risks.
- Information Technology should maintain and use policies, procedures, and processes to manage protection of HRM's network and related assets.
- Information Technology management and staff roles and responsibilities related to cybersecurity should be documented and understood.
- The network should be monitored and maintained to identify, document, and manage potential cybersecurity vulnerabilities and incidents.
- Network access (physical and logical) should be appropriately limited and monitored.
- HRM's management, staff, and elected officials should be provided adequate cybersecurity awareness training.

We used the NIST Cybersecurity Framework and NIST Special Publication (SP)800-53 to assess and conclude on our criteria. We did not complete a compliance audit against the frameworks.

Our audit period was January 1, 2021 – December 31, 2022. Information from outside the audit period was considered as necessary.

Our audit approach included: interviews with management and staff; review of internal policies and procedures; testing of key processes and controls; observation of activities, facilities, and operations; and examination of documents.

The audit was conducted in accordance with the Canadian Standards on Assurance and 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.

Appendix 1 – Recommendations and Management Responses

Recommendation 1

Information Technology management should assess resource needs to perform its cybersecurity duties and develop and implement plans to address the resource challenges.

Management Response

Agreed. IT Management will work with the CAO to determine the maturity level the organization wishes to obtain in the Cybersecurity practice and its adherence to the NIST Cybersecurity Framework. From this, current resourcing will be assessed, and any required resource needs articulated.

Recommendation 2

Information Technology management should complete the cybersecurity risk register and implement a process to periodically review and update.

Management Response

Agreed. IT management will implement a process for periodic review and updates to the cybersecurity risk register.

Recommendation 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.

Management Response

Agreed. 2022/2023 recommendations have been captured in the Cyber audit record document. Plans for risk treatment actions will be developed and results captured as they are addressed.

Recommendation 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.

Management Response

Agreed. IT Management has reviewed the 2018 threat risk assessment and all unaddressed relevant recommendations are captured in the 2022 and 2023 assessments. These will be addressed through actions on those reports' recommendations.

Recommendation 5

Information Technology management should develop and implement policies and related procedures to address key cybersecurity risks.

Management Response

Agreed. Policies, procedures, and guidelines will be Included in the remediation actions, where applicable.

Recommendation 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.

Management Response

Agreed. Vendor submissions are received today. IT Management will implement a process to ensure they are appropriately reviewed.

Recommendation 7

Information Technology management should replace physical locks at both datacentres immediately.

Management Response

Complete.

Recommendation 8

Information Technology management should implement a process to track keys and return to Corporate Security if no longer needed.

Management Response

Complete. Keys are controlled by Corporate Security, they have signed forms for the new keys for the DC's, only 3 are in existence.

Recommendation 9

Information Technology management should periodically review who has access to the datacentres and update as needed.

Management Response

Complete. Manager Enterprise Services & Infrastructure will request this report quarterly from Corporate Security until the ability to automate this report exists.

Recommendation 10

Information Technology management should implement a visitor log at all datacentre locations and require visitors be escorted by HRM IT management or staff.

Management Response

Complete. Visitor logs are now in place and visitors are required to sign in when escorted to either DC. Manager Enterprise Services & Infrastructure will review logs quarterly.

Recommendation 11

Information Technology management should document and communicate patch management procedures.

Management Response

Agreed. IT Management will document and communicate Polices, procedures and guidelines addressing vulnerability management for critical assets.

Recommendation 12

Information Technology management should determine and communicate an approved software list to IT staff who have the ability to download and install software.

Management Response

Agreed. IT Management will develop a process for determining approved software and create procedures and guidelines where appropriate.

Recommendation 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.

Management Response

Agreed. IT Management will audit gaps in the assignment of training.

Recommendation 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.

Management Response

Agreed. IT Management will audit the compliance reporting function available within the tool and will inform business units regarding employees who have not completed the training with requirements to have the training completed.

Recommendation 15

Information Technology management should determine next steps for employees who repeatedly fail to identify simulated phishing emails.

Management Response

Agreed. IT Management will audit the phishing reporting function available within the tool and provide appropriate feedback to employees who repeatedly fail to identify simulated phishing emails.

Recommendation 16

Information Technology management should develop and implement an asset management process to ensure assets are identified, inventoried, and managed.

Management Response

Agreed. IT Management will review the asset management process for gaps and augment processes where required.

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
Twitter: @Halifax AG