AUDITOR GENERAL

Halifax Regional Municipality

Halifax Regional Police Information Technology Audit – Public

February 2021

February 4, 2021

The following audit of **Halifax Regional Police Information Technology**, 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

Halifax Regional Police Information Technology Audit

HRP not effectively managing risks to its information technology systems

No documented process for managing patches to keep systems updated

OVERSIGHT

- **HRP's IT security needs significant improvements**
- **Limited progress related to security risk assessment completed in 2016-17**
- **No indication of how identified IT security risks will be mitigated**
- **HRP's existing IT policies outdated, and do not cover key IT security risks**
- **Board of Police Commissioners did not get adequate information on IT security consultant's report**

Security of Information and Assets

Aspects are adequate, but some gaps

No IT policies to determine which physical areas or information are sensitive

No policies for removable media such as USBs

No documented backup procedures

Due to the sensitive nature of IT, many of the areas we audited are reported in a separate in-camera report.

Most recommendations in the public and in-camera reports do not require an investment in IT infrastructure.

Audit Results

HRP is not effectively managing risks to its information technology systems and assets to adequately protect against internal and external threats. This report contains some of the findings from our audit in this area. There is also an in-camera report. The sections below are reported in greater detail in the in-camera report, along with sections on network operations, business continuity, and access. Given the sensitive nature of many IT topics, publicly reporting details of concerns identified could impact the safety and security of HRP operations.

Most of the recommendations in the public and in-camera reports do not require an investment in IT infrastructure to implement. Rather, they require updating policies to address modern IT issues and developing detailed processes to put policies into practice. Some recommendations may require commitment of funds to complete. It is important to recognize the potential costs of not investing could include greater risks to information security.

Our original planned audit of HRP IT security was delayed from spring 2018 to December 2019 because we wanted to give HRP time to implement some of the recommendations from a 2016-17 consultant report which assessed information security risks. The majority of the consultant's recommendations were still outstanding when we completed fieldwork in October 2020.

HRP IT operations fall into two areas: those entirely under HRP's management; and others where HRM ICT is involved. The scope of this audit was generally limited to areas which are entirely HRP's responsibility.

Oversight

Oversight of HRP's IT security needs significant improvements. A security risk assessment was completed in 2016-17 but there has been limited progress in addressing the concerns identified. Draft policies require substantial work to be put into operation. We also identified issues with the adequacy of information provided to the Board of Police Commissioners related to IT security.

The Board of Police Commissioners has administrative oversight of HRP's activities; however, we found HRP management did not always provide the Board with adequate information on IT security for the Board to carry out its duties. HRP's existing IT policies are outdated and do not cover key IT security risks. Policies, which address many of these risks, have been draft for over 18 months and there are no implantation plans.

We also found the staff member who manages HRP's covert systems is not supervised by someone with an IT background and has no reporting relationship with HRP's Chief Information Security Officer.

HRP IT has limited vendor service-level agreements, including with HRM ICT, to clearly establish roles and responsibilities. Without such agreements, important IT security tasks may not be completed.

Board of Police Commissioners given incorrect information on IT recommendations by HRP management

HRP management did not adequately brief the Board of Police Commissioners in 2017, following a consultant report on IT security.

We initially planned an audit of HRP IT security in Spring 2018 but decided to delay after HRP gave us a consultant report assessing IT security risks.

In July 2019, HRP management provided a detailed progress update on the semi-covert system recommendations to the Board of Police Commissioners. Management told the Board 13 of 67 recommendations in the semi-covert report were complete. We found:

- Six recommendations assessed as complete by HRP IT, were instead, outstanding.
- Another recommendation related to the Province of Nova Scotia; it should have been identified as not applicable to HRP IT.
- An eighth recommendation was outstanding because management decided not to move forward with it. However, it was presented to the Board as complete, rather than do not intend to implement.
- Five recommendations were complete at the time of the update in July 2019.

The Board was not briefed on the consultant's covert system recommendations. Up to October 2020, when we completed audit fieldwork, the Board had not been provided any information on those recommendations.

The Board has administrative oversight of HRP's activities, as defined by the Police Act. It is HRP management's responsibility to provide the Board with sufficient information to allow Board members to discharge their duties. Care must be taken to ensure information is complete and accurate.

Recommendation 1

Halifax Regional Police should implement a process to ensure only complete and accurate information on security of IT operations is provided to the Board of Police Commissioners.

Management Response

Agree. This recommendation will be actioned in the form of bi-monthly updates to BoPC commencing in April 2021. The frequency can be changed at the BoPC's discretion.

Insufficient oversight of covert system

One staff member manages covert IT systems, but is not supervised by someone with an IT background, and has no reporting relationship with HRP's Chief Information Security Officer (CISO).

HRP's CISO – hired in June 2018 – was not aware of the 2017 consultant report on IT security of HRP's covert operations until we asked for it during this audit. HRP IT staff had not informed the CISO this report existed. The CISO's job description notes *"The CISO would have direct responsibilities for the delivery of IT services…"* and *"… ability to act on behalf of the HRP Executive team in all IT operational aspects."* When we informed the CISO of the report on covert operations, in December 2019, we understand the CISO obtained a copy.

Recommendation 2

Halifax Regional Police should establish a reporting relationship between the Chief Information Security Officer and all staff with covert information technology security responsibilities.

Management Response

Agree. The employee will have a defined reporting relationship with the CISO by April 2021.

Risk management processes to protect information are not fully developed

Control Area	Current State – HRP	Why It Matters/ Risk
Information Security Risk Assessment What we were expecting: • completed information security risk assessment • periodically revisit	• Consultant completed an information security risk assessment. • It has not been refreshed since 2016-17. • No indication of risks to be mitigated or how, or work completed to date. • Have draft threat risk management policy but not approved and put into practice	• Existing risks have not been assessed to determine if action is needed. • If risk assessments are not re-visited periodically, new processes and associated risks may not be identified by management and therefore not prioritized and mitigated appropriately.
Information security risk treatment What we were expecting: • risk treatment plan identifies which risks to mitigate and how • key controls implemented to control identified risks are documented	• No plan detailing how risks will be mitigated. • No key controls that mitigate identified risks are documented.	• Risks may not get addressed or may not get addressed appropriately. • Difficult to determine how future changes impact risks

Planning to achieve information security objectives
 	
What we were expecting:
• Detailed plans to achieve information security objectives
	• Policies have been draft for more than 18 months.
	  ◦ No detailed plans to finalize and implement
	  ◦ New technology infrastructure may be needed to fully implement certain aspects.
		• Data loss or unauthorized access
		• Systems may not be available

Control Area	Current State – HRP	Why It Matters/ Risk
Defining the information security management system scope What we were expecting: • what processes and assets are included and who is responsible	• HRP working with HRM ICT to determine which IT systems and responsibilities will fall under HRP versus HRM ICT • No service-level agreement between HRP and HRM ICT	• If responsibilities and expectations are not clear and agreed upon by all parties, systems may not be protected, and the information security objectives not achieved.
Information security management system What we were expecting: • policies and processes to manage information systems and security	• Early phases of implementing information security management system • Have developed high-level draft policies ° Not implemented ° Substantial work needed to operationalize policies for HRP	• HRP's systems and data may be vulnerable to attack or compromise.
Leadership and commitment What we were expecting: • assigned project leader • an implementation plan for HRP's information security management system	• HRP does not have a system to manage its information security. ° There is a draft strategy document to develop a system. ° CISO is project leader ° No detailed plans to achieve strategy	• Without approval, may not have management support • An information security management system is fundamental to managing confidentiality, integrity, and availability of HRP's information assets.

Recommendation 3

Halifax Regional Police should update its information security risk assessment and document whether the identified risks will be mitigated, and how.

Management Response

Agree, the document will be updated, and the associated policy will be implemented by September 2021.

Recommendation 4

Halifax Regional Police should develop detailed plans for projects required to implement Halifax Regional Police's information security management system.

Management Response

Agree, HRP will develop and implement detailed plans for the required projects by December 2021.

Recommendation 5

Halifax Regional Police should finalize and implement its draft information technology security policies. This should include detailed guidance on how the policies will be applied to Halifax Regional Police information technology operations.

Management Response

Agree, HRP will finalize and implement the procedures and practices required to support the Information Security Management System as they apply to HRP operations by December 2021.

Recommendation 6

Halifax Regional Police should establish service-level agreements with IT service providers, including Halifax Regional Municipality's Information, Communication, and Technology division for Halifax Regional Police information technology systems and assets managed by Halifax Regional Municipality.

Management Response

Agree, HRP will finalize and establish those SLAs that are currently in draft as well as those that need to be created with the various parties by September 2021.

Key risks not appropriately addressed in existing policies

Control Topic	Current State – HRP	Why It Matters/ Risk
Information security policies should be established, approved, and communicated	• Existing policies are outdated and do not address key matters, such as access control and encrypting storage devices. • Draft policies address certain key risk areas but have not been approved, published and communicated to employees and relevant external parties.	• HRP employees may unknowingly put HRP systems and data at risk of attack or breach. • Breach of confidentiality • Privacy of data may not be protected • May not be able to recover from disaster ° Systems may not be available ° Operations may be affected
Information security policies should be reviewed regularly.	• Existing policies are outdated and do not address key risks. • Revised policies are draft and had not been approved as of October 2020.	• If policies are not regularly updated, they may no longer address existing security risks.

Control Topic	Current State – HRP	Why It Matters/ Risk

	• Policies often not specific to provide details of how policy should be implemented.
	• HRP IT management needs to establish guidance on how to operationalize policies at HRP.
	  ◦ Who can access information and systems, including physical access to buildings
	  ◦ Risks of mobile devices
	  ◦ Need to encrypt data
		For example, if a policy assigns responsibility to a certain role, and that role disappears due to organizational changes, the policy no longer holds anyone accountable, creating a risk the process will not be completed.
		• High-level policies may address risks but how policies are implemented will impact whether the risk is successfully mitigated.

Recommendation # 5 addresses finalizing and implementing draft policies.

Security of Information and Assets

Aspects of HRP's physical security over IT assets are adequate, but there are gaps which should be addressed. Datacentres have backup power supplies to maintain service during a power outage. HRP IT management told us security of IT equipment and environment for staff working from home is managed by HRM ICT. However, HRP IT has not assessed whether HRM's policies are sufficient for HRP's operations, in particular whether there are unique law enforcement considerations.

While certain aspects of HRP's IT operations have additional security measures, HRP IT has not implemented policies to address which physical areas or information are sensitive to determine what protections are needed. Additionally, there are no policies that address management of removable media, such as USB devices, which are riskier due to their portability. Existing policies do not cover secure deletion of sensitive information on damaged or surplus equipment. We also found IT equipment inventory assigned to the wrong vehicles; other equipment we checked was not included on an inventory list.

Physical and environmental security controls implemented, some gaps

Control Topic	Current State – HRP	Why it Matters/ Risk
Security areas should be established to protect sensitive information and systems.	• Draft policy defines levels of security (for example: public, internal, protected) ° Definitions only ° Has not been implemented to state level of security throughout various HRP locations	• Some internal information may require greater restrictions on who can access. • Without established security perimeters, inappropriate access to critical or sensitive information by unauthorized individuals may occur. This puts the security and integrity of the information at risk.
Protection from power failure	• HRP datacentres have uninterrupted power supplies. ° During audit fieldwork, HRP IT management told us the maintenance contract had not been renewed, meaning	• Without regular maintenance, the uninterrupted power

Control Topic	Current State – HRP	Why it Matters/ Risk
	maintenance could be not performed on the uninterrupted power supplies. ° However, in December 2020, management told us the contract was renewed in March 2020. • Uninterrupted power supplies allow equipment to run until a backup power supply starts. This helps ensure equipment continues to operate without interruption. • Management told us the buildings the datacentres are located in have generators. • For communication services, management told us both locations have network redundancy by having alternate sources of fibre for communications.	supply may not work when needed. ° Could lead to downtime in operations. ° Management should monitor contract renewals so HRP can get the services it pays for.
Taking equipment, information or software offsite	• Existing and draft policies do not address when equipment, information, or software can be taken offsite, or who must approve this.	• Equipment could be taken offsite when it should not be. • Policies tell employees what is acceptable and can be used to hold them accountable for their actions.

Recommendation 7

When Halifax Regional Police finalizes its draft policies, it should include which levels of physical security are required throughout Halifax Regional Police facilities.

Management Response

Agree, HRP will implement this recommendation by December 2021.

Policies do not address security of information stored on IT equipment

Control Topic	Current State – HRP	Why it Matters/ Risk
Secure data destruction – storage media	• Existing policies do not address secure data destruction. • Draft policy covers ensuring storage media has been securely overwritten before disposing of equipment. • Draft policy does not cover accidental disclosure or theft of sensitive information when damaged equipment is disposed of.	• Staff need to be aware of need to securely overwrite storage media before disposing of equipment. ° Should include damaged equipment since storage media may still be accessible ° Otherwise, sensitive information could be accidentally released.
Removable storage media considerations, including encryption	• Existing policies do not cover management of removable media, such as USBs. • Draft policies speak to a data classification scheme, including level of encryption required based on each classification. • Draft policies state removable media should not be used. ° This does not match the removable media practices currently in use, such as obtaining investigation information from the public on a USB.	• Removable media (i.e. USB drives) with sensitive data must be protected from unauthorized access to data. • For example, USBs are easy to lose or steal, due to their size. If the USB is not encrypted, the data on it would be readable to anyone who accesses it. • Devices from public or other agencies should be checked for viruses. • Encryption should be required.

Control Topic	Current State – HRP	Why it Matters/ Risk
Risks to offsite assets	• Key risks to attended and unattended equipment outside of the premises are not covered by existing or draft policies. ° No requirements for offsite equipment storage, use and communication. ° Policy does not require tracking offsite equipment.	• Offsite equipment has more risk associated with it. ° For example, if a laptop were left unattended in a car, it could be stolen.

Recommendation 8

Halifax Regional Police policies should address secure storage of information, including:

- secure data destruction when surplus or damaged equipment is disposed of;
- requirement for security of removable media; and
- protection and security of offsite equipment.

Management Response

- *Agree, HRP will update and implement its draft policies to reflect the components in this recommendation by June 2021.*

Inaccurate inventory lists

Control Topic	Current State – HRP	Why It Matters/ Risk

IT inventory should be maintained and updated	• Inventory lists were incomplete and inaccurate.
	• Management said they are identifying and classifying assets as part of an asset management project.
	  ◦ Does not include covert systems
	• HRP's asset list does not include:
	  ◦ Who is responsible for the asset – HRP or HRM ICT
	  ◦ All assets HRP is responsible for
		• Without accurate inventory, management cannot assess whether assets are appropriately protected from unauthorized access to the equipment or data.
		• Assets could go missing and HRP may not know.

Should know who has responsibility for IT assets	• HRP is responsible for: mobile data terminals, certain workstations, and surveillance equipment.
	  ◦ HRP has inventory lists for mobile data terminals and surveillance equipment.
	  ◦ An inventory list for the workstations HRP is responsible for was developed during the audit.
	• Inventory tracking for mobile data terminals in police vehicles is incomplete and inaccurate.
	  ◦ According to inventory listings, HRP has 162 mobile data terminals.
	  ◦ Of 21 terminals sampled:
	  ◦ Three were not on the inventory list.
	  ◦ Five were assigned to the wrong vehicle.
	  ◦ One was listed twice, in two different vehicles.
	• During the audit, the license expired for software used to track inventory. HRP did not take steps to get an inventory list before expiry.
		• Inventory lists, including location, allow an organization to keep track of its equipment.
		• Without accurate inventory lists, assets could go missing and HRP may not know.
		• If those assets contain confidential information, that information could be inappropriately disclosed.

Recommendation 9

Halifax Regional Police should update, and regularly maintain, its information technology asset lists.

Management Response

Agree, HRP will establish a process to regularly update and maintain its asset management list by April 2021.

No existing policy on teleworking

Control Topic	Current State – HRP	Why It Matters/ Risk
Consider teleworking sites – how to keep information safe	• For HRP employees working from home due to COVID-19, HRP IT management told us security of environment and equipment is HRM ICT's responsibility. ◦ HRM may have different requirements which may not cover HRP-specific risks.	• Employees working from home may access sensitive information. • Security of equipment and connection may be HRM's responsibility but HRP should have a policy stating how employees should secure their physical environment to prevent unauthorized persons from viewing data or accessing equipment and data. • This is particularly relevant given the sensitive nature of the information a police agency has.

Recommendation 10

Halifax Regional Police should assess Halifax Regional Municipality Information, Communication, and Technology division policies for teleworking to determine whether they are adequate for Halifax Regional Police purposes. Any concerns identified should be addressed in Halifax Regional Police policies.

Management Response

Agree, HRP will review and update its policies where additional measures are necessary for HRP purposes and reflect in its policies by April 2021.

Limited information technology security awareness training

Control Topic	Current State – HRP	Why it Matters/ Risk
IT security awareness training	• HRP does not provide HRP-specific IT security awareness training to its staff members.	• Training helps ensure employees are aware of their responsibilities to protect the organization's assets and systems, and the impact their actions could have.

Recommendation 11

Halifax Regional Police should provide its staff with regular information technology security awareness training, particularly given the sensitive nature of police operations.

Management Response

Agree, to date HRP employees have participated in security awareness training as provided by HRM. HRP will implement Security Awareness Training to meet police specific requirements by September 2021.

Information Technology System Operations

There were no documented processes for items such as patch management to keep systems updated, or backup procedures to ensure information can be recovered if there are issues.

Poor operational processes for systems

Control Topic	Current State – HRP	Why it Matters/ Risk
Documented operating procedures for IT systems	• No documented operating procedures for the maintenance of the two systems we audited, including patch management, change management, and backup procedures.	• Without documented procedures: ° Inconsistent approach to system changes across staff ° Nothing to guide new staff ° Important updates might be missed

Recommendation 12

Halifax Regional Police should develop and implement operating procedures to maintain its systems, including patch management, change management, and backup.

Management Response

Agree, HRP will develop detailed procedures for these areas by December 2021 and where infrastructure may be required, it will be identified along with associated timelines.

Background

Halifax Regional Police (HRP) provides policing services to certain areas within HRM, including Halifax, Dartmouth, Bedford, and areas between Bedford and the Sambro Loop.

The Halifax Board of Police Commissioners provides civilian oversight for Halifax Regional Police. The Nova Scotia Police Act gives the Board the authority to provide *"the administrative direction, organization and policy required to maintain an adequate, effective and efficient police department".*

In 2018, HRP hired a Chief Information Security Officer (CISO). The CISO is the senior IT resource for HRP and acts as its liaison for IT-related matters with Halifax Regional Municipality.

HRP uses information technology that is supported by HRP IT staff, as well as HRM IT staff.

The Strategic Technology Integration Unit reports to the CISO. This unit is responsible for support, maintenance and implementation of certain HRP-specific information systems and applications.

HRP's Technical Surveillance Unit, part of the Criminal Investigations Division, has its own IT systems and network to support certain investigations. A technician with an IT background manages this equipment. The unit reports to the Superintendent, Criminal Investigation Division.

About the Audit

We completed a performance audit of Halifax Regional Police Information Technology

The purpose of the audit was to determine whether HRP appropriately manages risks to its information technology systems. Our role is to express an independent audit opinion of this area.

The objective of the audit was to determine whether HRP manages risks to information technology systems and assets to ensure systems and data are adequately protected from internal and external threats.

We developed the criteria for this audit. These were discussed with, and accepted as appropriate by, management of Halifax Regional Police.

1. HRP management should have processes to ensure information systems security risks are appropriately identified, addressed, and managed.

2. HRP management should implement key controls appropriate to manage information systems security risks.

Our audit period was from February 1, 2019 to January 31, 2020. We considered information outside the audit period as we deemed necessary.

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

In carrying out our work, we considered HRP's overall IT environment. Where specific testing was necessary, we examined two semi-covert systems, as well as the covert network, since testing every system HRP IT is responsible for was not practical.

HRP management told us they use ISO/IEC standard 27001 to guide their IT security operations. This standard speaks to the requirements to implement and maintain an information security management system. Many of these requirements are fundamental to IT security and similar points can be found in other authoritative sources. We used ISO 27001 to evaluate HRP's IT security practices.

This audit 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 Control 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

Halifax Regional Police should implement a process to ensure only complete and accurate information on security of IT operations is provided to the Board of Police Commissioners.

Management Response

Agree. This recommendation will be actioned in the form of bi-monthly updates to BoPC commencing in April 2021. The frequency can be changed at the BoPC's discretion.

Recommendation 2

Halifax Regional Police should establish a reporting relationship between the Chief Information Security Officer and all staff with information technology security responsibilities.

Management Response

Agree. The employee will have a defined reporting relationship with the CISO by April 2021.

Recommendation 3

Halifax Regional Police should update its information security risk assessment and document whether the identified risks will be mitigated, and how.

Management Response

Agree, the document will be updated, and the associated policy will be implemented by September 2021.

Recommendation 4

Halifax Regional Police should develop detailed plans for projects required to implement Halifax Regional Police's information security management system.

Management Response

Agree, HRP will develop and implement detailed plans for the required projects by December 2021.

Recommendation 5

Halifax Regional Police should finalize and implement its draft information technology security policies. This should include detailed guidance on how the policies will be applied to Halifax Regional Police information technology operations.

Management Response

Agree, HRP will finalize and implement the procedures and practices required to support the Information Security Management System as they apply to HRP operations by December 2021.

Recommendation 6

Halifax Regional Police should establish service-level agreements with IT service providers, including Halifax Regional Municipality's Information, Communication, and Technology division, for Halifax Regional Police information technology systems and assets managed by Halifax Regional Municipality.

Management Response

Agree, HRP will finalize and establish those SLAs that are currently in draft as well as those that need to be created with the various parties by September 2021.

Recommendation 7

When Halifax Regional Police finalizes its draft policies, it should include which levels of physical security are required throughout Halifax Regional Police facilities.

Management Response

Agree, HRP will implement this recommendation by December 2021.

Recommendation 8

Halifax Regional Police policies should address secure storage of information, including:

- secure data destruction when surplus or damaged equipment is disposed of;
- requirement for security of removable media; and
- protection and security of offsite equipment.

Management Response

Agree, HRP will update and implement its draft policies to reflect the components in this recommendation by June 2021.

Recommendation 9

Halifax Regional Police should update, and regularly maintain, its information technology asset lists.

Management Response

Agree, HRP will establish a process to regularly update and maintain its asset management list by April 2021.

Recommendation 10

Halifax Regional Police should assess Halifax Regional Municipality Information, Communication, and Technology division policies for teleworking to determine whether they are adequate for Halifax Regional Police purposes. Any concerns identified should be addressed in Halifax Regional Police policies.

Management Response

Agree, HRP will review and update its policies where additional measures are necessary for HRP purposes and reflect in its policies by April 2021.

Recommendation 11

Halifax Regional Police should provide its staff with regular information technology security awareness training, particularly given the sensitive nature of police operations.

Management Response

Agree, to date HRP employees have participated in security awareness training as provided by HRM. HRP will implement Security Awareness Training to meet police specific requirements by September 2021.

Recommendation 12

Halifax Regional Police should develop and implement operating procedures to maintain its systems, including patch management, change management, and backup.

Management Response

Agree, HRP will develop detailed procedures for these areas by December 2021 and where infrastructure may be required, it will be identified along with associated timelines.

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: hrmauditorgeneral.ca
Twitter: @Halifax AG