

**2024**  
**Report of the Auditor General  
to the Nova Scotia  
House of Assembly**



**Cybersecurity Readiness in  
Healthcare**



**Performance Audit**  
**Independence • Integrity • Impact**

**Intentionally Left Blank**

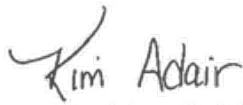
October 22, 2024

Honourable Danielle Barkhouse  
Speaker  
House of Assembly  
Province of Nova Scotia

Dear Madam Speaker:

I have the honour to submit herewith my Report to the House of Assembly under Section 18(2) of the *Auditor General Act*, to be laid before the House in accordance with Section 18(4) of the *Auditor General Act*.

Respectfully,



**Kim Adair, FCPA, FCA, ICD.D**  
Auditor General of Nova Scotia

5161 George Street  
Royal Centre, Suite 400  
Halifax, NS B3J 1M7  
Telephone: (902) 424-5907  
[www.oag-ns.ca](http://www.oag-ns.ca)

 [/company/oag-ns](https://www.linkedin.com/company/oag-ns)

 [@OAG\\_NS](https://twitter.com/OAG_NS)

 [/OAGNS](https://www.facebook.com/OAGNS)

 [@nsauditorgeneral](https://www.instagram.com/nsauditorgeneral)

**Intentionally Left Blank**

# Table of Contents

1	Cybersecurity Readiness in Healthcare .....	7
	Reference Guide – Key Findings and Observations.....	9
	Recommendations and Responses .....	11
	Questions Nova Scotians May Want to Ask.....	15
	Definitions .....	16
	Background .....	18
	Shared responsibility, but minimal accountability between DHW, NSH and CSDS ..	22
	Deficiencies in Key Digital Health Network Controls.....	28
	Failure to Appropriately Manage Cybersecurity Risks by DHW, NSH and CSDS ....	32
	Appendix I: Reasonable Assurance Engagement Description and Conclusions .....	40

**Intentionally Left Blank**

# Cybersecurity Readiness in Healthcare

## Departments of Health and Wellness, Cyber Security and Digital Solutions, and Nova Scotia Health

### Key Messages

- The Departments of Health and Wellness, Cyber Security and Digital Solutions, and Nova Scotia Health are not effectively providing cybersecurity for Nova Scotia's digital health network.
- The same three government entities share responsibility for the digital health network, but there is a lack of accountability for cybersecurity.
- Critical deficiencies identified in key network controls.
- Audit reveals pervasive tolerance for accepting cybersecurity risk and failure to manage ongoing risks.
- We will follow up to evaluate progress on sensitive technical observations not publicly reported within one year.

### Why We Did This Audit

- Digital networks are increasingly prevalent in delivery of patient care and hold some of Nova Scotians' most sensitive health information.
- Serious cyber-attacks on healthcare organizations that disrupt patient care, disable networks, and steal sensitive information are becoming frequent in Canada.
- Nova Scotia's government has prioritized expanding digital technologies to transform health care.
- Without robust cybersecurity, Nova Scotia's digital health network is at serious risk.

### Shared responsibility, but minimal accountability between DHW, NSH and CSDS

- Governance framework set out in shared service agreement abandoned in 2021-22. Once governance committees abandoned, cybersecurity initiatives stalled.
- Department of Health and Wellness (DHW), as the executive sponsor of the health system, failing to establish priority for cybersecurity across the digital health network.
- Nova Scotia Health (NSH), as the business owner of major clinical systems, failing to establish meaningful accountability for cybersecurity.
- Cyber Security and Digital Solutions (CSDS), as a service provider, may raise cybersecurity concerns, but has no authority to take action to protect the digital health network.
- Key performance indicators to measure and track cybersecurity still not established.

### Deficiencies in Key Digital Health Network Controls

- Key network control weaknesses have been confidentially communicated to DHW, NSH and CSDS.
- Cybersecurity policies and standards are not regularly reviewed and updated.
- Digital asset inventory listings are unreliable and incomplete.
- Cybersecurity training program not mandatory for all users of the digital health network.

## Failure to Appropriately Manage Cybersecurity Risks by DHW, NSH and CSDS

- Heavy reliance on vendors to provide digital assets, but contracts are not required to include cybersecurity protections and contract management is lacking.
- The Architecture Review Board allows projects to connect to the digital health network without meeting established cybersecurity standards.
- NSH policy lets health decision makers decide which cybersecurity standards to apply on a case-by-case basis, leading to high levels of risk acceptance.
- Testing showed cybersecurity risks frequently accepted.
- Ongoing risk management of digital assets once connected to the digital health network is weak and unreliable, hampered by a lack of role clarity and a lack of accountability mechanisms.
- Control weaknesses in cybersecurity risk management results in the accumulation of cybersecurity risk across the digital health network.




## Reference Guide – Key Findings and Observations

Paragraph	Key Findings and Observations
<i>Background</i>	
1.1	Background
1.7	Nova Scotia’s digital health network and those responsible for upkeep
1.12	DHW and NSH legally required to protect personal health information on the digital health network
1.17	Nova Scotia uses the National Institute of Standards and Technology (NIST) Cybersecurity Framework as a guide
1.18	Focus and approach of our Audit
<i>Shared responsibility, but minimal accountability between DHW, NSH and CSDS</i>	
1.23	IT Governance framework set out in shared service agreement abandoned in 2021 - 2022
1.30	Disbandment of oversight after the Health Leadership Team (HLT) was established in 2021
1.32	IT system business owners allowed to bypass cybersecurity risk assessments
1.34	OAG identified projects in the network that may not have completed cybersecurity assessments
1.35	Disbanding IT governance committees leaves cybersecurity work stranded
1.38	Lack of IT governance gives minimal accountability for cybersecurity during rapid expansion of the digital health network
1.42	Lack of emphasis for cybersecurity governance stalls NSH’s enterprise risk activity
1.44	NSH not reporting as required by enterprise risk policy
1.48	Serious cybersecurity enterprise risks not effectively identified
1.52	Key performance indicators still not established for managing cybersecurity
<i>Deficiencies in Key Digital Health Network Controls</i>	
1.56	Improvements to Key Network Controls needed
1.59	Cybersecurity policies and standards are not regularly updated and inconsistently applied
1.64	Digital asset inventory listings are unreliable and incomplete
1.66	Cybersecurity training not mandatory for all users during our audit period
1.69	Detect, respond and recover are essential for cybersecurity readiness
1.70	Ineffective analysis of some cybersecurity incidents
1.71	CSDS followed response plan during MOVEit breach
<i>Failure to Appropriately Manage Cybersecurity Risks by DHW, NSH and CSDS</i>	
1.73	Risk management is important for maintaining cybersecurity
1.74	Widespread reliance on vendors to deliver digital health projects
1.76	Health sector vendor IT contracts not required to include cybersecurity provisions
1.78	Management of vendor IT contracts is still lacking, needs significant improvement
1.81	Architecture Review Board to review and approve technology projects
1.84	Testing shows most projects do not fully comply with the ARB process
1.85	ARB pressured to rush projects
1.87	Projects tested did not meet cybersecurity standards after completing the ARB process
1.88	ARB allows projects to connect to the digital health network without meeting cybersecurity standards
1.89	ARB not effectively managing cybersecurity risk
1.90	Testing shows health decision makers frequently accept cybersecurity risks

Paragraph	Key Findings and Observations
1.94	CSDS tracks some cybersecurity risks but do not use these to manage risks
1.95	Weaknesses in managing cybersecurity risk identified
1.96	Unaddressed risk persists in important clinical system
1.98	Ongoing risk management in digital assets is weak and unreliable
1.100	Lack of clarity for roles and responsibilities weakens risk management
1.103	Lack of accountability mechanisms weakens risk management











## Recommendations and Responses

Recommendation	Department Response	
<p><b>Recommendation 1.1</b> We recommend DHW, NSH and CSDS establish an effective IT governance framework to manage cybersecurity across the digital health network.</p> <p><i>See paragraph 1.41</i></p>	<p>While we agree with the recommendation, it is important to acknowledge part of the audit review period was during the COVID-19 pandemic and a time of significant organizational change at NSH and DHW. These two events disrupted normal governance and operating procedures and may have impacted the audit findings. Many changes have been implemented in the year following the audit period.</p> <p>DHW, NSH and CSDS recognize the need for a framework to strengthen shared governance of digital health operations. They will establish appropriate forum(s) for review and oversight of ongoing cybersecurity initiatives, and work to align that forum with evolving digital health governance. The implementation will utilize an iterative approach, with governance being introduced in stages.</p>	<p> Department Agrees</p> <p> <b>Target Date for Implementation:</b> January 2025</p>
<p><b>Recommendation 1.2</b> We recommend NSH complete cybersecurity assessments for the remaining projects approved under Business Risk Acceptance Forms (BRAAF) process and take appropriate action on cyber risks identified.</p> <p><i>See paragraph 1.41</i></p>	<p>NSH recognizes the importance of cybersecurity assessments. Temporary solutions were put in place to support the COVID-19 response. NSH and CSDS will jointly review the list and prioritize the active solutions by January 2025. Cyber security assessments will then be actioned, starting with those that are highest priority, by April 2025. It is expected that the cyber assessments on active solutions will be completed by October 2026.</p>	<p> Department Agrees</p> <p> <b>Target Date for Implementation:</b> January 2025 April 2025 October 2026</p>
<p><b>Recommendation 1.3</b> We recommend NSH follow the enterprise risk management policy for identified cybersecurity risks.</p> <p><i>See paragraph 1.47</i></p>	<p>The audit period also coincided with Nova Scotia's emergency response to the COVID-19 pandemic. The pandemic strained Nova Scotia's healthcare systems. To ensure the health and safety of all Nova Scotians, NSH altered care, regular administrative duties and requirements to ensure a complete focus on pandemic response.</p> <p>NSH has established a renewed focus on ERM and will comply with the stated policy in this area.</p>	<p> Department Agrees</p> <p> <b>Target Date for Implementation:</b> April 2025</p>
<p><b>Recommendation 1.4</b> We recommend NSH improve its risk identification process to identify patterns of risks across multiple technology projects and enter them as enterprise risks.</p> <p><i>See paragraph 1.51</i></p>	<p>NSH and CSDS will put a joint process in place to identify patterns. When patterns meet a risk threshold, they will be entered into the risk registry.</p>	<p> Department Agrees</p> <p> <b>Target Date for Implementation:</b> March 2025</p>
<p><b>Recommendation 1.5</b> We recommend DHW, NSH and CSDS establish key performance indicators for cybersecurity across the digital health network.</p> <p><i>See paragraph 1.55</i></p>	<p>DHW, CSDS and NSH will establish KPIs for cybersecurity across the digital health network. They will liaise with other jurisdictions in Canada to validate the Provinces KPI's against key performance indicators being used by other jurisdictions.</p>	<p> Department Agrees</p> <p> <b>Target Date for Implementation:</b> February 2025</p>









## Recommendations and Responses

Recommendation	Department Response	
<p><b>Recommendation 1.6</b> We recommend DHW, NSH and CSDS immediately review the technical reports by our cybersecurity expert and prepare and implement appropriate and detailed action plans. The Office of the Auditor General will follow up in a year to assess progress.</p> <p><i>See paragraph 1.58</i></p>	<p>CSDS and NSH have begun to review the technical reports and will work with DHW and vending partners to mitigate risks iteratively based on risk profile and best practices.</p> <p>During the scope of the audit, there was an agreement with the OAG that any critical vulnerabilities identified through their technical review would be shared with CSDS, NSH and DHW. One risk was identified through this agreement and immediate action was taken.</p>	<p> Department Agrees</p> <p> <b>Target Date for Implementation:</b> Ongoing</p>
<p><b>Recommendation 1.7</b> We recommend DHW, NSH and CSDS conduct a comprehensive policy and standards review and develop a maintenance schedule to provide for regular, timely review.</p> <p><i>See paragraph 1.63</i></p>	<p>DHW, CSDS, and NSH will review cybersecurity standards and policies. There will also be an emphasis on defining and implementing a sustainable process of reviews. Accountability for a given policy or standard will be included in the review.</p>	<p> Department Agrees</p> <p> <b>Target Date for Implementation:</b> October 2025</p>
<p><b>Recommendation 1.8</b> We recommend DHW, NSH and CSDS implement a consistent inventory management procedure so sufficient and appropriate cybersecurity information is maintained for all network connected assets.</p> <p><i>See paragraph 1.65</i></p>	<p>CSDS, NSH and DHW will evaluate existing inventories of network connected assets and seek to create a consistent inventory management process by October 2025. CSDS, NSH and DHW will investigate automated tools and resources to support this work including auditing functionality by October 2026.</p>	<p> Department Agrees</p> <p> <b>Target Date for Implementation:</b> October 2025 October 2026</p>
<p><b>Recommendation 1.9</b> We recommend DHW, NSH and CSDS establish a program of auditing of network connected assets.</p> <p><i>See paragraph 1.65</i></p>	<p>See 1.8</p>	<p> Department Agrees</p> <p> <b>Target Date for Implementation:</b> October 2025 October 2026</p>
<p><b>Recommendation 1.10</b> We recommend DHW and NSH make cyber awareness training both available and mandatory for all users of the digital health network and track compliance.</p> <p><i>See paragraph 1.68</i></p>	<p>NSH has established a cybersecurity training program including mandatory attendance for new hire onboarding. Establishment of this program occurred outside the audit period.</p> <p>NSH will require mandatory completion of cybersecurity training by all employees by October 2025 and will verify compliance annually.</p> <p>DHW cybersecurity awareness training course was available effective March 2024. Its completion is mandatory for all employees and managers and compliance will be verified annually.</p>	<p> Department Agrees</p> <p> <b>Target Date for Implementation:</b> Complete</p>
<p><b>Recommendation 1.11</b> We recommend DHW, NSH and CSDS complete and comply with existing standards for security logs and back-up restore process.</p> <p><i>See paragraph 1.69</i></p>	<p>In alignment with Recommendation 1.7, DHW, CSDS and NSH will review existing standards for security logs and back-up restore processes by October 2025. Once the standard is reviewed, parties will work together to monitor and manage compliance as required.</p>	<p> Department Agrees</p> <p> <b>Target Date for Implementation:</b> October 2025</p>

## Recommendations and Responses

Recommendation	Department Response	
<p><b>Recommendation 1.12</b> We recommend CSDS track and analyze all types of cybersecurity incidents.</p> <p style="text-align: right;"><i>See paragraph 1.70</i></p>	<p>CSDS currently has a cyber incident tracking system in place. CSDS will review the existing cybersecurity incident tracking program and set criteria for which security incidents should be tracked.</p>	<p> Department Agrees</p> <p> <b>Target Date for Implementation:</b> March 2025</p>
<p><b>Recommendation 1.13</b> We recommend DHW, NSH and CSDS implement minimum cybersecurity contract provisions for all technology projects connecting to the digital health network.</p> <p style="text-align: right;"><i>See paragraph 1.80</i></p>	<p>The audit period also coincided with Nova Scotia's emergency response to the COVID-19 pandemic. The pandemic strained Nova Scotia's healthcare systems. To ensure the health and safety of all Nova Scotians, NSH altered care delivery systems in a rapid fashion including the emergency implementation of several key systems.</p> <p>CSDS and DHW will continue to maintain a Security Obligations contract schedule that includes recommended cybersecurity provisions for technology projects. Delivery teams take a risk-based approach to tailor these provisions.</p> <p>NSH has established standardized cyber contract schedules. Establishment of these schedules occurred outside the audit period.</p>	<p> Department Agrees</p> <p> <b>Target Date for Implementation:</b> Complete</p>
<p><b>Recommendation 1.14</b> We recommend DHW, NSH and CSDS amend existing contracts to include the minimum cybersecurity contract provisions, or where not possible, take appropriate action to mitigate the impact of the missing provisions.</p> <p style="text-align: right;"><i>See paragraph 1.80</i></p>	<p>NSH, DHW and CSDS are not able to impose additional security requirements on current contracts unilaterally. Vendors would need to agree to any change in terms.</p> <p>Security requirements for existing contracts will be reviewed at the time of renewal or as new contracts are negotiated.</p>	<p> Department Disagrees</p> <p> <b>Target Date for Implementation:</b> Ongoing</p>
<p><b>Recommendation 1.15</b> We recommend DHW, NSH and CSDS insist on vendor compliance with contract terms at all stages of a contract, including validating vendor compliance with the minimum cybersecurity provisions.</p> <p style="text-align: right;"><i>See paragraph 1.80</i></p>	<p>DHW, NSH and CSDS will continue to work with vendors to ensure they meet minimum cyber security provisions. By December 2025, a formal process and related procedure will be established which is part of overall contract management processes.</p>	<p> Department Agrees</p> <p> <b>Target Date for Implementation:</b> December 2025</p>
<p><b>Recommendation 1.16</b> We recommend DHW, NSH and CSDS adhere strictly to the ARB process and only allow projects to connect to the digital health network that have completed ARB and meet cybersecurity standards.</p> <p style="text-align: right;"><i>See paragraph 1.89</i></p>	<p>The audit period also coincided with Nova Scotia's emergency response to the COVID-19 pandemic. The pandemic strained Nova Scotia's healthcare systems. To ensure the health and safety of all Nova Scotians, NSH altered care delivery systems in a rapid fashion including the emergency implementation of several key systems.</p> <p>NSH has established procedures to ensure that all open cyber risks are addressed in a timely manner. Establishment of these procedures occurred outside the audit period.</p> <p>CSDS, NSH and DHW will collaborate to define a digital assurance process to ensure solutions meet cybersecurity standards.</p>	<p> Department Agrees</p> <p> <b>Target Date for Implementation:</b> October 2025</p>

## Recommendations and Responses

Recommendation	Department Response
<p><b>Recommendation 1.17</b> We recommend DHW and NSH stop all ad hoc business risk acceptance practices and implement clear risk tolerance thresholds tied to cybersecurity standards and aligned with the custodian's responsibilities under the <i>Personal Health Information Act</i>.</p> <p><i>See paragraph 1.97</i></p>	<p>CSDS, NSH and DHW will continue to take a holistic view of risk that balances the risk of urgent patient care and cyber security. The partners will work collectively to review existing processes for the management of cyber risks that fall outside defined risk tolerance thresholds. This work will align with evolving governance structures (recommendation 1.1).</p> <p>  Department Agrees   <b>Target Date for Implementation:</b> October 2025         </p>
<p><b>Recommendation 1.18</b> We recommend DHW and NSH establish an accountability mechanism to verify planned risk mitigations are completed for all digital assets.</p> <p><i>See paragraph 1.97</i></p>	<p>NSH has established procedures to ensure that open cyber risks for IT assets currently monitored by NSH are assessed, and where relevant, have planned mitigations. Establishment of these procedures occurred outside the audit period.</p> <p>DHW will develop procedures to ensure cyber risks are assessed, and where relevant, are addressed in a timely manner.</p> <p>  Department Agrees   <b>Target Date for Implementation:</b> June 2025         </p>
<p><b>Recommendation 1.19</b> We recommend DHW, NSH and CSDS establish standard operating procedures with clear roles and responsibilities to provide for ongoing maintenance and management of cybersecurity risks in clinical medical devices, facilities and clinical applications.</p> <p><i>See paragraph 1.103</i></p>	<p>CSDS, NSH and DHW will review and enhance risk monitoring and reporting processes, clearly identify accountability for addressing risk and communication of asset risk to business owners for deployment of digital solutions including medical devices.</p> <p>  Department Agrees   <b>Target Date for Implementation:</b> December 2025         </p>
<p><b>Recommendation 1.20</b> We recommend DHW, NSH and CSDS establish a mechanism to hold business owners accountable for maintaining security patches and updates in digital assets.</p> <p><i>See paragraph 1.103</i></p>	<p>CSDS, NSH and DHW will review patch management processes and clearly identify accountability for maintaining security patches and updates in digital assets.</p> <p>  Department Agrees   <b>Target Date for Implementation:</b> March 2025         </p>

## Questions Nova Scotians May Want to Ask

1. What will Health and Wellness, Cyber Security and Digital Solutions, and Nova Scotia Health do to improve cybersecurity for the digital health network?
2. Will Health and Wellness, Cyber Security and Digital Solutions, and Nova Scotia Health enforce cybersecurity standards for technology connecting to the digital health network?
3. What will Health and Wellness, Cyber Security and Digital Solutions, and Nova Scotia Health do to bring meaningful accountability for cybersecurity risk to the digital health network?
4. Will Health and Wellness, Cyber Security and Digital Solutions, and Nova Scotia Health prioritize strengthening cybersecurity foundations before continuing to expand technology use?
5. Will Health and Wellness, Cyber Security and Digital Solutions, and Nova Scotia Health take action to address the vulnerabilities and risky technologies currently connected to the digital health network?
6. How safe is my health information on the digital health network?



## Definitions

**Architecture:** The structure, design, and overarching principles of an Information Technology (IT) system and its components, including hardware and software.

**Architecture Review Board:** A group of Government experts who review and provide comment on new IT and system deployments before approval.

**Business Owner:** The clinical division owner responsible for individual assets (computers, applications) in the healthcare system; i.e. the *business owner* of an MRI machine is the imaging division of Nova Scotia Health.

**Clinical systems/assets:** Systems and assets used for patient care in clinical or medical settings.

**Cybersecurity:** Security measures that ensure confidentiality, integrity, and access to information stored digitally in data centers or in a cloud environment. Cybersecurity protects computer systems, networks, and data from unauthorized access, attacks, and damage like viruses, hackers and other malicious activities.

**Database:** Collects, organizes, and stores large volumes of data (digital assets, logs, risks, etc.) in columns and tables for fast and efficient retrieval, update, and management.

**Digital assets:** Hardware items (desktop computers, printers, etc.), software items (applications, digital tools, active directory, etc.) and infrastructure (servers, routers, firewalls, etc.) that connect to a network.

**Digital Health Network:** A network connecting all *digital assets* (see above) used by Nova Scotia Health, the Department of Health and Wellness, and third-party users which contains identifiable information and the personal health information of Nova Scotians.

**Firewall:** A network security device which monitors and controls incoming and outgoing network traffic based on predetermined security rules to authenticate users.

**Information Technology (IT):** A broad term that encompasses computers, networks, software, and other technology that stores, retrieves, transmits, and manipulates data.

**Malware:** Malicious software designed to harm or exploit computer systems. Common types of malware include viruses, worms, trojans, *ransomware* (see below), and spyware.

**NIST framework:** National Institute of Standards and Technology's five-step framework (Identify, Protect, Detect, Respond, Recover) that helps organizations better manage and improve the security of their digital environment.



## Definitions, *continued*

**One Person One Record (OPOR):** An electronic health record set to launch in 2025 that will make a patient's medical data and medical history available across the healthcare system to health professionals, beginning in acute care facilities.

**Patch:** A piece of software designed to fix, update or improve the functionality or security of a computer program or supporting data. Patches are crucial to address known vulnerabilities and maintain cybersecurity.

**Personal Health Information:** Identifiable and sensitive information about a person that is collected, used, or disclosed during healthcare service delivery; we refer to this type of information in the report as *patient health data*.

**Phishing:** An attack by email that tricks recipients into divulging sensitive information, such as usernames, passwords, or financial details.

**Security logging:** A digital record of all detailed activities on a file and in a system by user, including the time, location, permissions given, and authentication methods employed.

**Supply Chain:** The provision of goods and services provided by organizations, usually third parties, by contract.

**Threat Actors:** Cyberthreat actors or malicious actors are individuals or groups that intentionally cause harm to digital devices or systems.

**Vulnerability:** A weakness or flaw in a system's design, implementation, or operation which could be exploited to compromise the confidentiality, integrity, or availability of the system.

# 1 Cybersecurity Readiness in Healthcare

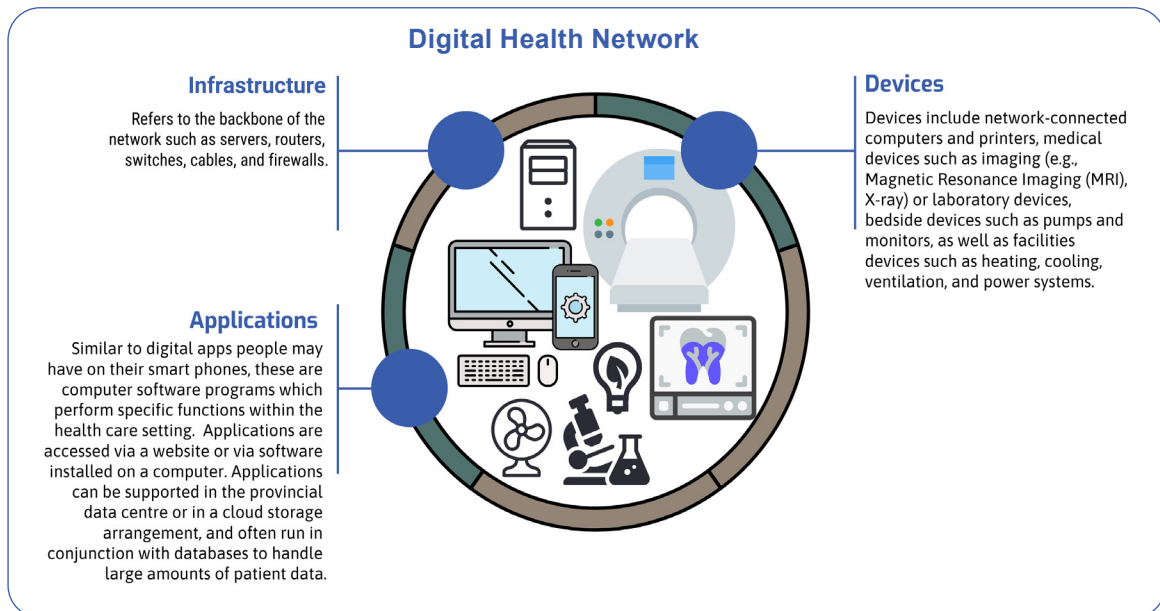
## Departments of Health and Wellness, Cyber Security and Digital Solutions, and Nova Scotia Health

### Background

- 1.1 Cybersecurity attacks have caused significant damage in Canadian health care organizations and to patients in recent years, with organizations sometimes taking months to recover. Impacts to health care from two recent publicly reported cyber attacks (in the province of Newfoundland and Labrador in 2021 and to a group of hospitals in Southwestern Ontario in 2023) include:
  - Serious disruptions to patient care
  - Disabling of digital networks preventing communications and normal workflows
  - Disabling of access to patient records
  - Theft of patient and employee personal information.
- 1.2 The consequences of an attack are very serious, and Nova Scotians have an interest in knowing whether the digital health network supporting their healthcare system and storing their private information is secure and ready to defend from cyber attack.
- 1.3 At the same time, the digital transformation of health care is a significant component of Nova Scotia's current *Action for Health* plan. Digital goals and strategies are set out under multiple solutions of government's plan for health care. Recent investments in digital technologies are significant. In 2023, the government announced a contract for \$365 million with Oracle Cerner to implement the long-awaited One Person One Record electronic medical record system. The YourHealthNS App, and Virtual Care NS are other examples of technology innovation and investment in the digital health network developed at an approximate cost of \$30 million, plus ongoing operating costs.
- 1.4 The current strategic focus on technology investments and the general increase of digital technology in health care leads to a corresponding need for maintenance, upkeep, and strong cybersecurity foundations to protect the growing and complex digital health network. Technology, such as computer hardware and software, requires continuous support once it is connected to a network. Ongoing maintenance and upkeep of this technology is significant, as these elements need constant monitoring, testing, updating, and resolving vulnerabilities.
- 1.5 We previously completed two relevant information technology audits in 2018 and 2019. Those audits found issues with governance, contract management, risk management, and with deploying new technology without assessing cybersecurity risks. Our 2019 financial report also raised concerns about cybersecurity management across government and at NSH.
- 1.6 During a Public Accounts Committee (PAC) meeting on June 9, 2021 to discuss fraud risk management and cybersecurity, senior government management made strong statements indicating they understand the cybersecurity risks facing the digital health network and gave specific assurance of the commitment to managing cybersecurity risks.

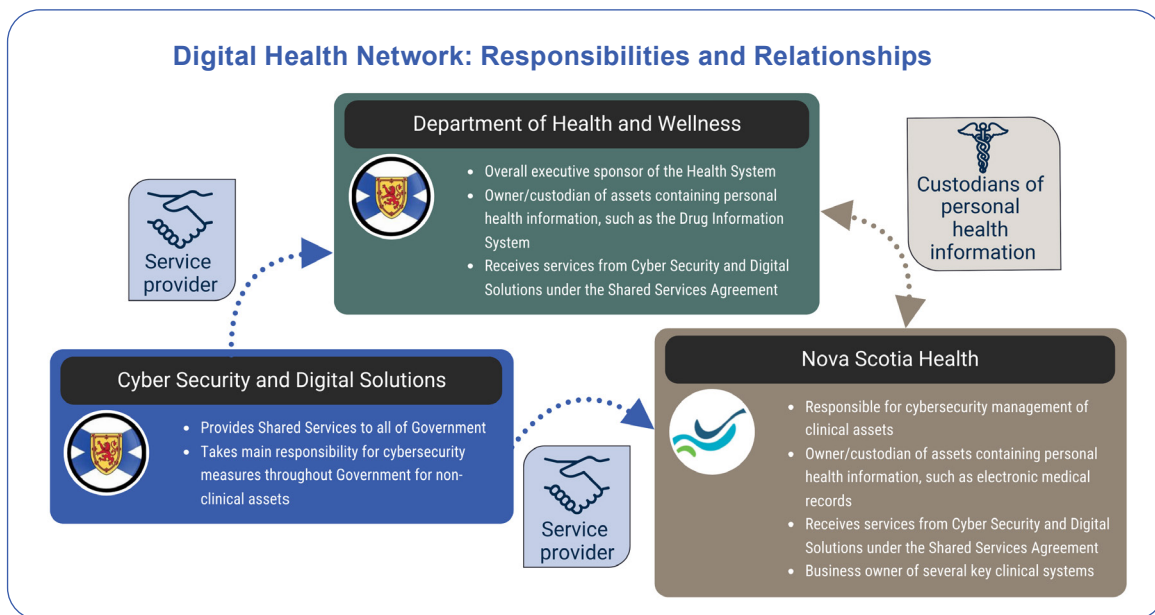
## ➔ Nova Scotia's digital health network and those responsible for upkeep

- 1.7 The digital health network uses technology for communication and to generate, transmit and organize data and information used by staff and clinicians providing health care. The digital health network is made up of a complex collection of connected digital assets managed under a Shared Services Agreement between the Department of Health and Wellness (DHW), Nova Scotia Health (NSH), the Department of Cyber Security and Digital Solutions (CSDS) and the IWK Health Centre (IWK). Assets can be broadly grouped into three categories: devices, infrastructure, and applications.



Source: Office of the Auditor General of Nova Scotia

- 1.8 DHW provides a key source of funding and leadership to the health sector, including a statutory responsibility to establish technical and informational requirements and standards for health-information systems. Under the terms of the Shared Services Agreement, it is described as the “overall executive sponsor of the Health System” and is also a client of the Department of Cyber Security and Digital Solutions. DHW is the business owner of several key clinical systems such as the Drug Information System, the Panorama electronic public health information system, and the health data repository which collects personal health data from multiple sources across the network.
- 1.9 NSH was established in 2015 following the amalgamation of regional district health authorities. NSH provides direct healthcare services to patients via hospitals, clinics, and other care sites. NSH is responsible for more than 13,000 connected clinical medical devices, hundreds of connected facility devices, and over 400 software applications, most used in clinical medical settings.
- 1.10 CSDS was created in 2023 and was previously known as the Nova Scotia Digital Service as part of the Department of Service Nova Scotia and Internal Services. CSDS provides technology and cybersecurity expertise to government and the health sector. CSDS provides the facilities and support for the digital health network’s main data center and approximately 20,000 provincially owned computers deployed to the digital health network. CSDS also provides the infrastructure which gives most users access to the digital health network.



Source: Office of the Auditor General of Nova Scotia

- 1.11 The *Personal Health Information Act* states that custodians (health professionals or health organizations who collect and use personal health information during the provision of healthcare services) are responsible for the safekeeping of personal health information.

### **DHW and NSH legally required to protect personal health information on the digital health network**

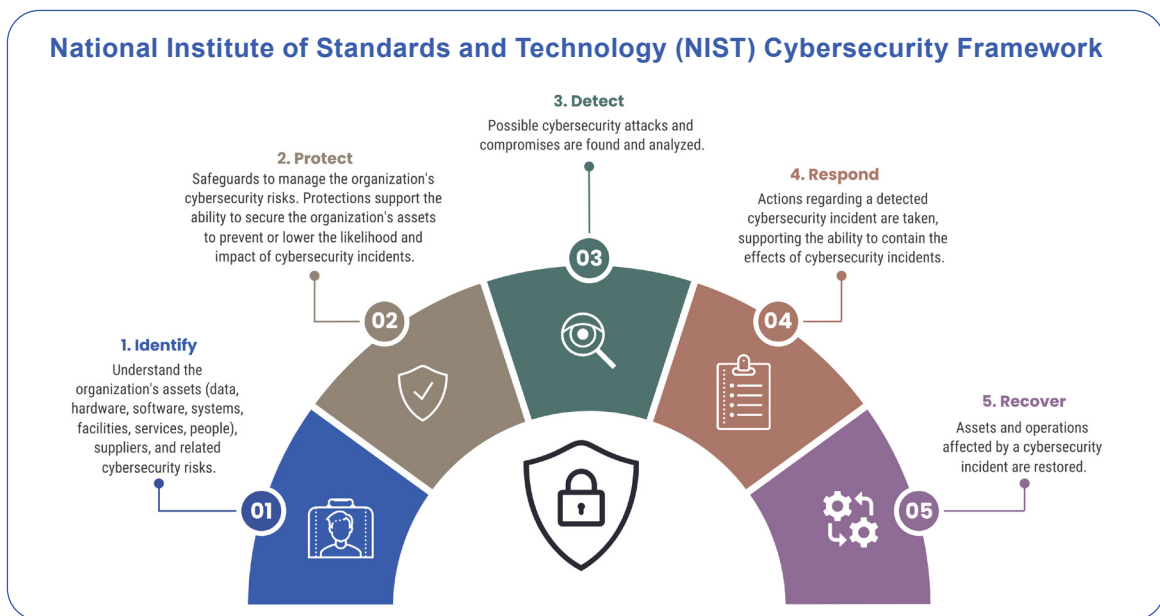
- 1.12 The *Personal Health Information Act* sets out additional responsibilities once a custodian decides to use digital technologies and introduces personal health information to a digital platform. The custodian must maintain reasonable security for digital systems and the accompanying regulations set out further requirements to protect network infrastructure, hardware, and software. The regulations require the custodian to create and maintain written policies to support and enforce the implementation of security for the digital systems it decides to use.
- 1.13 DHW and NSH are both custodians of personal health information for specific digital assets. For example, the DHW is the custodian of the Drug Information System used by pharmacies and doctors to obtain and record information about prescriptions prescribed and dispensed across the province. NSH is the custodian of a wide range of digital systems that directly engage with personal health information, such as electronic medical records, digital systems for cancer care, patient screening, patient monitoring, microbiology, and diagnostic imaging, etc.
- 1.14 DHW and NSH are also the custodians of many systems that depend on structures and technologies owned or operated by other parties. For example, many of the systems used by NSH may be hosted by a vendor in a cloud or rely on components owned and maintained by a vendor. Much of the digital health network also depends on CSDS-owned and operated hardware and software technologies and infrastructure. Vendors and CSDS are not custodians under the *Personal Health Information Act*.
- 1.15 Even though these other network components may not directly touch personal health information, or they may be owned and operated by another party, their presence on the network can impact the

security status of the network. Because of the interconnected nature of the digital health network and because personal health information flows throughout the network, it is the custodians who have ultimate responsibility for security of the network under the *Personal Health Information Act*.

- 1.16 As custodians, DHW and NSH are under a regulatory requirement to enforce the implementation of cybersecurity to protect personal health information on the digital health network. Vulnerabilities in some parts of the digital health network increase the risk for the whole network and personal health information on the network cannot be protected without reasonable and effective cybersecurity extended to all components of the digital health network. The results of this audit raise worrying questions about DHW and NSH compliance with their statutory responsibilities which may be of interest to Nova Scotia’s Privacy Commissioner, the regulator responsible for the *Personal Health Information Act*.

**Nova Scotia uses NIST Cybersecurity Framework as a guide**

- 1.17 The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Commerce Department. NIST publishes a cybersecurity framework which sets out industry standards, guidelines and practices into activity areas to help organizations implement or improve cybersecurity. Nova Scotia uses the NIST framework for cybersecurity as a guideline when developing programs and processes. The framework covers a broad range of technology and organizational structures. Accountability for cybersecurity becomes increasingly more difficult to manage as a network or organization grows and increases in complexity. We used the NIST framework’s themes and intent when developing the criteria and testing for this audit.



Source: Office of the Auditor General of Nova Scotia

**Focus and approach of our Audit**

- 1.18 We recognize that our audit work could expose specific cybersecurity weaknesses within the Nova Scotia digital health network. As a result, any technical findings that could provide an opportunity to threat actors have not been reported publicly. Instead, sensitive observations



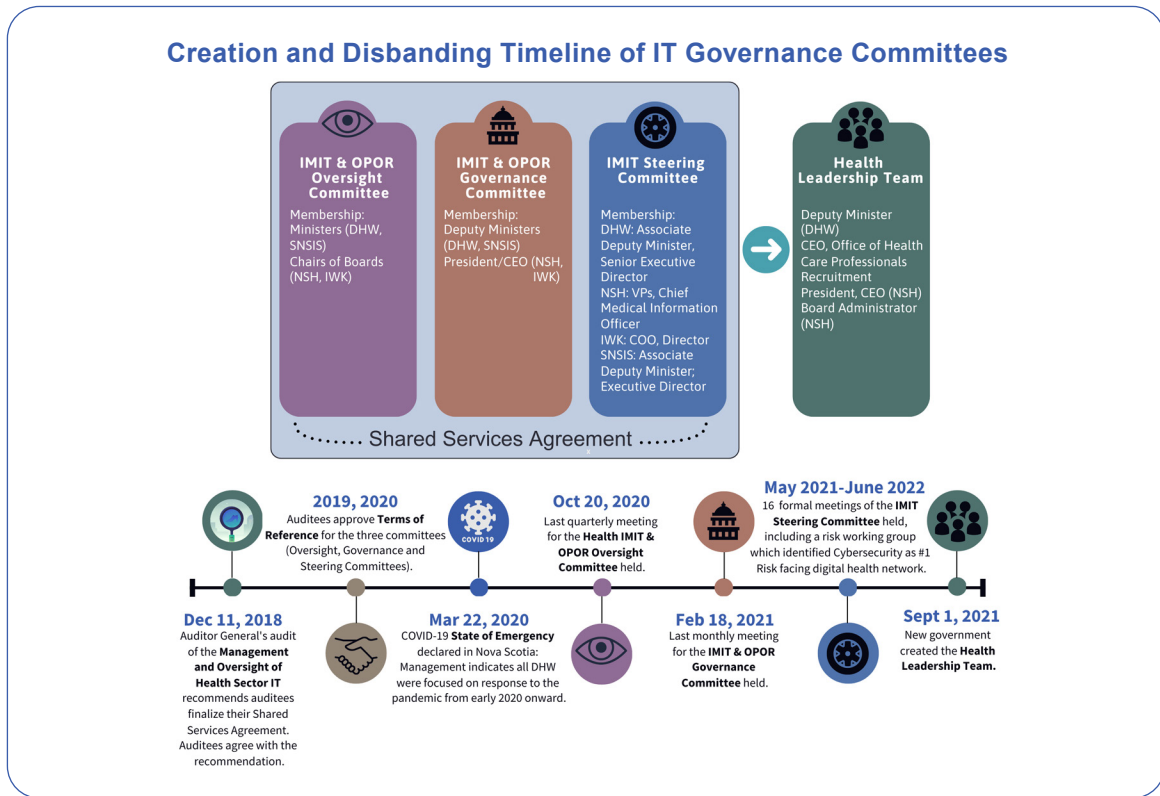
have been directly provided to management, along with the detailed findings of our independent cybersecurity expert.

- 1.19 The scope of this audit is broad, covering the underlying infrastructure relied on by the digital health network for processing, storage, routing, and security, as well as instances of cloud infrastructure, software, hardware devices, and third-party providers who deploy products or services within NSH's digital health network. We excluded the IWK as an auditee, but it also relies on aspects of the network operated by CSDS, DHW, and NSH.
- 1.20 Our work included reviewing policies and procedures and examining data and records. Staff and management of the three entities were also interviewed. With the assistance of a contracted cybersecurity expert, we also tested key technical aspects of the assets and systems to determine the status and effectiveness of cybersecurity for the digital health network.
- 1.21 The audit period was from April 1, 2021, to June 1, 2023. Where necessary, testing was extended beyond the audit period.
- 1.22 Throughout the audit we refer to established cybersecurity standards for the digital health network, which are specific technical standards published by CSDS intended to protect Nova Scotia's digital health network from cyber-attack. Where we refer to non-compliance with established cybersecurity standards, it is a reference to not following these published standards.

## Shared responsibility, but minimal accountability between DHW, NSH and CSDS

### IT Governance framework set out in shared service agreement abandoned in 2021 – 2022

- 1.23 A shared services agreement for providing information technology services to the healthcare sector is used in Nova Scotia. Shared services agreements are used to achieve efficiency of scale, consistency across departments, and the development of areas of expertise.
- 1.24 Within the healthcare sector, shared services are implemented through a three-tier IT governance structure, consisting of agreements between DHW, NSH and CSDS. With multiple parties involved in decision-making and service and program delivery, it is critical to clearly define responsibilities among the parties.
- 1.25 The timeline below outlines the creation and disbanding of IT governance committees set out in the Shared Services Agreement, as outlined in the committees' Terms of References.



Source: Office of the Auditor General of Nova Scotia

- 1.26 Our audit of the Management and Oversight of Health Sector Information Technology in 2018 recommended the auditees finalize their Shared Services Agreement. The recommendation was accepted by all three auditees. The auditees approved Terms of Reference for the three committees in 2019 and 2020.
- 1.27 Management reported the Oversight Committee last met on October 20, 2020, and the Governance Committee last met on February 18, 2021. Management said all DHW teams were focused on COVID-19 response as a top priority from early 2020 onward, and other COVID-19 response-focused management meetings took priority. Management reported it has no records of meetings held for the Health IMIT Oversight and Governance Committees, such as agendas, attendance, meeting minutes, or records of decisions during our audit period.
- 1.28 IMIT Steering Committee minutes show 16 meetings occurred between May 2021 and June 2022, including reports from a cybersecurity risk working group. The IMIT Steering Committee discussed, identified, and prioritized risks to the digital health network, and formal minutes and attendance were recorded. At the time, cybersecurity was identified as the number one risk facing the digital health network.
- 1.29 Although the IMIT Steering Committee met between 2021 and 2022, our review noted instances where a focus on accountability was lacking. For example, on four separate occasions DHW was asked to provide representatives for cybersecurity risk management activities. However, DHW did not provide representatives. Furthermore, a DHW position called Director of Risk was eliminated during a reorganization. The minutes also reflect uncertainty as participants questioned who would take long-term responsibility for management of IT controls.

**Disbandment of oversight after HLT was established in 2021**

- 1.30 The Health Leadership Team (HLT), consisting of the Deputy Minister of the Department of Health and Wellness, CEO of the Office of Health Care Professionals Recruitment, the President and CEO of NSH, and the Board Administrator for NSH, was created to lead the healthcare system on September 1, 2021. HLT did not continue with the IT governance structure set out in the Shared Services Agreement and the IMIT Steering Committee last met on June 1, 2022.
- 1.31 Once discontinued, the IT governance committee structure was not replaced. The Risk Working Group that reported to the IMIT Steering Committee also stopped its work once the committee stopped meeting. Currently, there is no evidence of any IT governance for the digital health network. IT governance has essentially been abandoned.

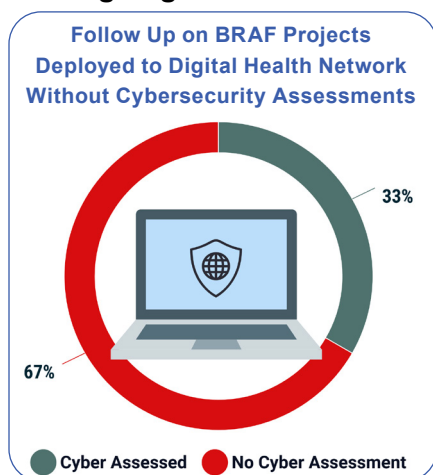
**IT system business owners allowed to bypass cybersecurity risk assessments**

- 1.32 A key cybersecurity decision noted in the IMIT Steering Committee minutes was the decision to stop using the Business Risk Acceptance Form (BRAf) process in December 2021. The BRAf process allowed business owners to decline cybersecurity risk assessments in the development and deployment of technology assets. Allowing business owners to decline risk assessments results in technology assets deployed to the digital health network without any assessment of the risk the technology posed to the existing network or how the technology asset could be vulnerable to cyber-attack.
- 1.33 We can see in the January 12, 2022 minutes of the IMIT Steering Committee, the technology expertise from CSDS played a role in securing agreement with DHW and NSH to stop using the BRAf process. We can also see in the minutes where CSDS started follow up on projects approved under the BRAf process to assess vulnerabilities. This demonstrated an aspect of accountability for cybersecurity across the digital health network at that time.

**OAG identified projects in the network that may not have completed cybersecurity assessments**

- 1.34 In March 2024, we asked for an update about the initiative to follow up on the projects approved under the BRAf process. CSDS management indicated that their last follow-up on the issue was completed in 2022 and showed assessments were only completed for 33% of the projects where cybersecurity assessments were declined using the BRAf process.

**Disbanding IT governance committees leaves cybersecurity work stranded**



- 1.35 When asked why the cybersecurity assessments have not been completed, CSDS management told us under the Shared Service Agreement, accountability for completing security risk assessments on new or major changes to existing applications rests with business owners such as NSH.

Source: Office of the Auditor General of Nova Scotia



- 1.36 The role of CSDS under the shared services agreement is as service provider and source of expertise for advisory and strategic services. CSDS cannot direct healthcare decision makers, even if cybersecurity issues are identified, or if a proposed technology does not comply with the cybersecurity standards of government. Multiple CSDS staff indicated the lack of enforcement role as a limitation on CSDS.
- 1.37 The IMIT Steering Committee provided a formal forum to advance accountability, with all partners on equal footing. However, once the IMIT Steering Committee stopped meeting, the forum was no longer available. In addition, formalized accountability for the remaining identified projects approved without any cybersecurity assessment stopped.

### **Lack of IT governance gives minimal accountability for cybersecurity during rapid expansion of the digital health network**

- 1.38 CSDS's role in bringing technology expertise and cybersecurity standards to the governance of the digital health network is an important check and balance for health decision makers. Having an effective check and balance is important, as the government moves to rapidly transform health care through technology investments.
- 1.39 DHW management confirmed they did not engage in any cybersecurity risk management activities during the audit period. The DHW is the executive sponsor of the health system, which identified cybersecurity as its top IT risk in 2021. There is an expectation for DHW to be a leader in terms of tone and emphasis on the importance of cybersecurity with the government's objective to transform health care through technology. In 2023, the Health Transformation Office at the Department of Health and Wellness put forward a plan and proposal for a new health sector digital governance structure.
- 1.40 We reviewed the proposed DHW plan on digital health governance. The proposed governance structure eliminates representation of CSDS from the senior leadership decision table and eliminates the IMIT Steering Committee established under the shared services agreement. By not including cybersecurity expertise at all levels of decision making, there is a risk of foregoing the important check and balance it can provide. However, this proposed structure has not yet been implemented and there is currently no IT governance for the digital health network.
- 1.41 While HLT is providing leadership, it is not equivalent to the IT governance structures set out in the shared services agreement. Without IT governance, there is no foundation for reporting and accountability for cybersecurity. While there were initial efforts at IT governance and accountability, those Committees have been abandoned.

#### **Recommendation 1.1**

We recommend DHW, NSH and CSDS establish an effective IT governance framework to manage cybersecurity across the digital health network.

#### **Health and Wellness, Nova Scotia Health and Cyber Security and Digital Solutions Response:**

While we agree with the recommendation, it is important to acknowledge part of the audit review period was during the COVID-19 pandemic and a time of significant organizational change at NSH and DHW. These two events disrupted normal governance and operating procedures and may have impacted the audit findings. Many changes have been implemented in the year following the audit period.

DHW, NSH and CSDS recognize the need for a framework to strengthen shared governance of digital health operations. They will establish appropriate forum(s) for review and oversight of ongoing cybersecurity initiatives, and work to align that forum with evolving digital health governance. The implementation will utilize an iterative approach, with governance being introduced in stages. Target Date: January 2025.

### **Recommendation 1.2**

We recommend NSH complete cybersecurity assessments for the remaining projects approved under Business Risk Acceptance Forms (BRAAF) process and take appropriate action on cyber risks identified.

**Nova Scotia Health Response:** NSH recognizes the importance of cybersecurity assessments. Temporary solutions were put in place to support the COVID-19 response. NSH and CSDS will jointly review the list and prioritize the active solutions by January 2025. Cyber security assessments will then be actioned, starting with those that are highest priority, by April 2025. It is expected that the cyber assessments on active solutions will be completed by October 2026. Target Date: January 2025, April 2025, October 2026.

### **Lack of emphasis for cybersecurity governance stalls NSH's enterprise risk activity**

- 1.42 NSH's Enterprise Risk Management Policy (ERM) is designed to be consistent with generally accepted global enterprise risk management standards. Its goal is to identify, communicate and effectively manage existing and emerging risks. The policy sets out a commitment to ensuring risk management practices are embedded into all processes and operations to drive consistent, effective, and accountable action, and decision making in management practice and Board governance oversight.
- 1.43 However, we identified that updates of cybersecurity risks in NSH's enterprise risk register stopped in 2022 after the IMIT Steering Committee stopped meeting.

### **NSH not reporting as required by enterprise risk policy**

- 1.44 NSH's Enterprise Risk Management Policy requires the Board to review and approve Action plans to address risk mitigations and opportunities, as well as review and approve management's risk register and risk assessment results annually. It requires the President and CEO to provide status updates to the Board twice per year, senior leaders to report to their Vice President on the status of assigned risk items twice per year, and Directors to report to their senior leader on the status of assigned risk items quarterly.
- 1.45 We examined the reporting under NSH's Enterprise Risk Management Policy for a sample of identified enterprise risks. We observed no Board review and approval of risk action plans as required by the ERM policy. However, a summary risk register was presented to the Board administrator. We observed no status updates to the Board from the President/CEO and no reports to Vice Presidents from senior leaders on assigned items as required by the ERM policy. In total we observed only 12% (7/60) of reporting required by the policy was completed during the audit period.
- 1.46 Our analysis found only 50% (2/4) of risks were the subject of a formalized risk management plan and they were the only ones in the sample to document in the risk register any tangible action taken to mitigate the risks.

- 1.47 Overall, NSH is not following their enterprise risk management policy and reporting is not done as required for cybersecurity risks. This increases the risk of systematic cybersecurity issues going unaddressed which weakens the overall security of the digital health network.

### Recommendation 1.3

We recommend NSH follow the enterprise risk management policy for identified cybersecurity risks.

**Nova Scotia Health Response:** The audit period also coincided with Nova Scotia's emergency response to the COVID-19 pandemic. The pandemic strained Nova Scotia's healthcare systems. To ensure the health and safety of all Nova Scotians, NSH altered care, regular administrative duties and requirements to ensure a complete focus on pandemic response.

NSH has established a renewed focus on ERM and will comply with the stated policy in this area. Target Date: April 2025.

### Serious cybersecurity enterprise risks not effectively identified

- 1.48 We also found gaps in the risks captured in NSH's enterprise risk management system. Management told us there is no obligation for project personnel to submit risks to the enterprise risk register. Management also confirmed there is currently no process to identify trends of the same or similar risks across multiple projects. This opens the significant possibility legitimate enterprise risks are not captured and entered in the enterprise risk management system.
- 1.49 Our review of project documentation found multiple instances where the same risk was identified within many projects, and where project owners accepted risks with comments indicating it was an organization-wide risk.
- 1.50 For example, one of the recurring theme risks we identified affected more than a dozen individual projects. The same risk was also flagged by NSH-hired consultants as a cybersecurity gap and is reflected in NSH's internal documentation. For these reasons, we would expect it to be identified as an enterprise risk. The risk was never entered into the enterprise risk register. As a result, the risk has never been formally reported to the Board of NSH, even in a summary form.
- 1.51 We asked for an update on the status of this risk and management's response was a plan must be developed, and discussions are ongoing. In our opinion, this is an inadequate response to a serious risk identified almost four years ago. Recurring themes of risks being accepted at the individual project level should alert those charged with governance, but it does not.

*Recurring themes not identified as enterprise risk.*

### Recommendation 1.4

We recommend NSH improve its risk identification process to identify patterns of risks across multiple technology projects and enter them as enterprise risks.

**Nova Scotia Health Response:** NSH and CSDS will put a joint process in place to identify patterns. When patterns meet a risk threshold, they will be entered into the risk registry. Target Date: March 2025.

## Key performance indicators still not established for managing cybersecurity

- 1.52 We found no evidence of key performance indicators (KPIs) planned or in use to measure or evaluate cybersecurity within the digital health network by any of the organizations we audited. Identifying and tracking key performance indicators are a best practice approach for any organization looking to track progress and improvement over time.
- 1.53 KPIs for cybersecurity may include indicators such as numbers of cybersecurity vulnerabilities on the network, the number of assets connected to the digital health network that do not meet cybersecurity standards, or the number of vendor contracts that do not contain sufficient cybersecurity requirements. The organization could then track those indicators over time to measure their progress in improving cybersecurity.
- 1.54 The absence of KPIs measuring cybersecurity for the digital health network was identified as a weakness as early as 2020 in an internal report. We also observed within an NSH internal document, draft cybersecurity metrics were completed but not put in place.
- 1.55 The issues identified throughout this report demonstrate an urgent need to adopt KPIs for accountability and to measure progress leading to better outcomes for the digital health network.

### **Recommendation 1.5**

We recommend DHW, NSH and CSDS establish key performance indicators for cybersecurity across the digital health network.

**Health and Wellness, Nova Scotia Health and Cyber Security and Digital Solutions Response:** DHW, CSDS and NSH will establish KPIs for cybersecurity across the digital health network. They will liaise with other jurisdictions in Canada to validate the Provinces KPI's against key performance indicators being used by other jurisdictions. Target Date: February 2025.

## Deficiencies in Key Digital Health Network Controls

### Improvements to Key Network Controls needed

- 1.56 The NIST cybersecurity framework outlines the use of network controls in pursuit of improving cybersecurity. Network controls in this context refers to a wide range of actions, requirements and practices to help manage cybersecurity risks.
- 1.57 We identified weaknesses in several key network controls. In addition, our cybersecurity expert conducted extensive penetration and network control testing, producing multiple technical reports.
- 1.58 To protect the sensitivity of the information, details of these reports and identified deficiencies in network controls were provided to management separately. As a result, we have significant concerns about cybersecurity across the digital health network and for this reason will follow up on this observation sooner than normal, in one year.

### **Recommendation 1.6**

We recommend DHW, NSH and CSDS immediately review the technical reports by our cybersecurity expert and prepare and implement appropriate and detailed action plans. The Office of the Auditor General will follow up in a year to assess progress.

**Health and Wellness, Nova Scotia Health and Cyber Security and Digital Solutions Response:** CSDS and NSH have begun to review the technical reports and will work with DHW and vending partners to mitigate risks iteratively based on risk profile and best practices.

During the scope of the audit, there was an agreement with the OAG that any critical vulnerabilities identified through their technical review would be shared with CSDS, NSH and DHW. One risk was identified through this agreement and immediate action was taken. Target Date: Ongoing.

### **Cybersecurity policies and standards are not regularly updated and inconsistently applied**

- 1.59 In general, cybersecurity standards are a set of techniques, controls and processes organizations can implement to achieve and maintain security within the organization. However, there is no internationally recognized framework which organizations must follow.
- 1.60 While the province uses the NIST cybersecurity framework as guidance, the province also uses internally developed policies and standards to implement cybersecurity in the digital health network. We reviewed policies and standards pertaining directly to cybersecurity or containing objectives to increase cybersecurity awareness. We observed weaknesses in the application and management of policies and standards, including outdated policies not undergoing regular reviews and updates. Additionally, we identified policies dating back to former district health authorities on technology topics within NSH.
- 1.61 One of the basic ways to protect an organization against cybersecurity threats is through a policy foundation that is regularly updated and standards which reflect best practice. This is not currently occurring within the health digital network.
- 1.62 Lastly, we observed policies do not consistently apply for all auditees. Under the NSH Information Security Policy, NSH decides which security standards will be applied. NSH management told us this means standards are applied on an ad hoc, project-by-project basis. This policy language allows NSH to opt-out of cybersecurity standards set by CSDS.
- 1.63 Based on our review, cybersecurity policies are fragmented, out-of-date and reside in numerous locations. This confusing policy foundation makes cybersecurity readiness difficult to oversee.

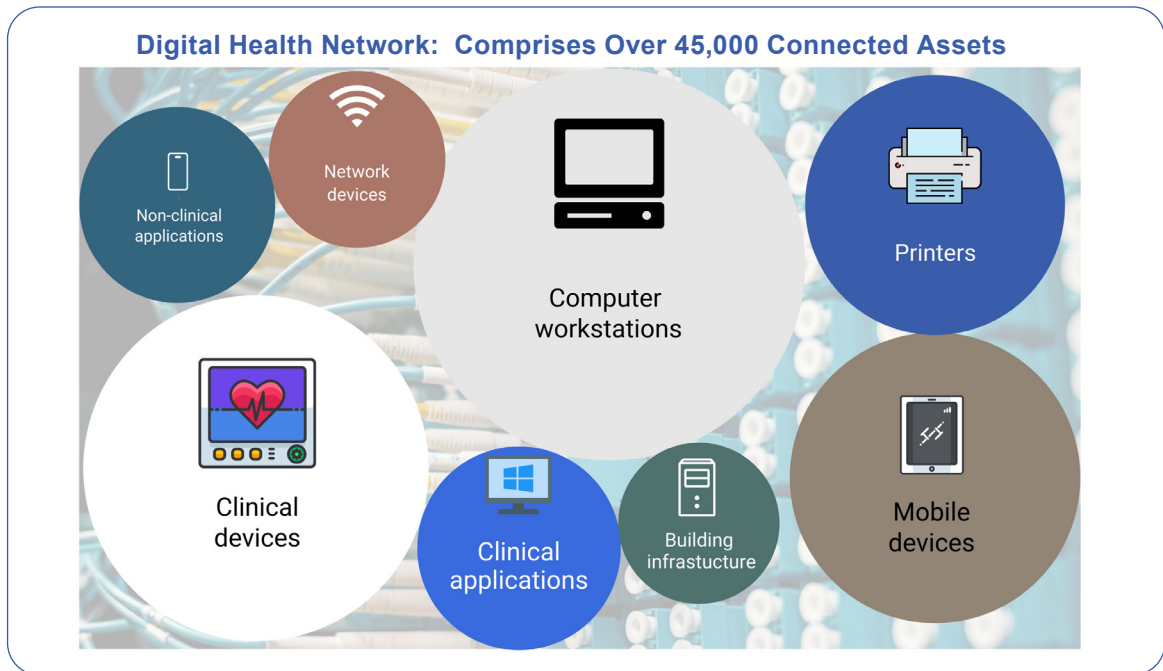
#### **Recommendation 1.7**

We recommend DHW, NSH and CSDS conduct a comprehensive policy and standards review and develop a maintenance schedule to provide for regular, timely review.

**Health and Wellness, Nova Scotia Health and Cyber Security and Digital Solutions Response:** DHW, CSDS, and NSH will review cybersecurity standards and policies. There will also be an emphasis on defining and implementing a sustainable process of reviews. Accountability for a given policy or standard will be included in the review. Target Date: October 2025.

### **Digital asset inventory listings are unreliable and incomplete**

- 1.64 The NIST cybersecurity framework identifies managing assets using inventories of hardware, software, services, and data as a key area of activity to manage cybersecurity risks. Being able to identify and control what is connected to the digital health network is an important foundation for cybersecurity. Knowing what is connected and how it is connected allows for auditing and management of cybersecurity.



Source: Office of the Auditor General of Nova Scotia

1.65 We found a lack of consistent procedures for collecting and maintaining information, a lack of coordination between those maintaining the lists and those working with the assets, and a lack of validation of information included in the lists. Our testing found digital asset inventory listings in their current state are unreliable and incomplete.

**Recommendation 1.8**

We recommend DHW, NSH and CSDS implement a consistent inventory management procedure so sufficient and appropriate cybersecurity information is maintained for all network connected assets.

**Health and Wellness, Nova Scotia Health and Cyber Security and Digital Solutions Response:** CSDS, NSH and DHW will evaluate existing inventories of network connected assets and seek to create a consistent inventory management process by October 2025. CSDS, NSH and DHW will investigate automated tools and resources to support this work including auditing functionality by October 2026. Target Date: October 2025, October 2026.

**Recommendation 1.9**

We recommend DHW, NSH and CSDS establish a program of auditing of network connected assets.

**Health and Wellness, Nova Scotia Health and Cyber Security and Digital Solutions Response:** See 1.8

 **Cybersecurity training not mandatory for all users during our audit period**

1.66 An example of one network control we examined is cybersecurity awareness for network users. User behavior poses a significant risk to the network, as users are targeted by attackers. Training users to spot phishing attempts, how to report them, and to generally never put their credentials into a weblink, is needed to protect the digital health network.



- 1.67 We examined NSH's cyber awareness training module implemented to educate and make users aware of the risks and the importance of their behavior in protecting against cyber-attack. However, there are serious gaps in the delivery of training to users. The online module is offered to NSH employees but not to external users and is not mandatory.
- 1.68 Management confirmed there was no mandatory cyber awareness training offered to DHW employees during our audit period. However, recent mandatory cybersecurity specific training has been rolled out across government, including to DHW (excluding NSH). Management also confirmed there is no cyber awareness training offered to external users of the digital health network.

### Recommendation 1.10

We recommend DHW and NSH make cyber awareness training both available and mandatory for all users of the digital health network and track compliance.

**Health and Wellness and Nova Scotia Health Response:** NSH has established a cybersecurity training program including mandatory attendance for new hire onboarding. Establishment of this program occurred outside the audit period.

NSH will require mandatory completion of cybersecurity training by all employees by October 2025 and will verify compliance annually.

DHW cybersecurity awareness training course was available effective March 2024. Its completion is mandatory for all employees and managers and compliance will be verified annually. Target Date: Complete.

## Detect, respond and recover are essential for cybersecurity readiness

- 1.69 Cyber incidents can take various forms, such as a threat actor gaining access to a digital health network and causing damage by interfering with access to a system or by stealing data. The NIST cybersecurity framework places an emphasis on organizations to detect, respond and recover from cyber incidents. We reviewed standards and practices in this area including security logging and back-up restore process.

### Recommendation 1.11

We recommend DHW, NSH and CSDS complete and comply with existing standards for security logs and back-up restore process.

**Health and Wellness, Nova Scotia Health and Cyber Security and Digital Solutions Response:** In alignment with Recommendation 1.7, DHW, CSDS and NSH will review existing standards for security logs and back-up restore processes by October 2025. Once the standard is reviewed, parties will work together to monitor and manage compliance as required. Target Date: October 2025.

## Ineffective analysis of some cybersecurity incidents

- 1.70 CSDS has a Major Incident Management process that sets out roles and responsibilities and formalizes processes for managing major incidents. A major incident is defined as an incident that has or could pose a significant impact to critical services demanding a response beyond routine incident management. CSDS tracks major incidents through a centralized site. Incidents not defined as major incidents are tracked in a different system that does not allow for analysis, review, and reporting.

### **Recommendation 1.12**

We recommend CSDS track and analyze all types of cybersecurity incidents.

**Cyber Security and Digital Solutions Response:** CSDS currently has a cyber incident tracking system in place. CSDS will review the existing cybersecurity incident tracking program and set criteria for which security incidents should be tracked. Target Date: March 2025.

#### **CSDS followed response plan during MOVEit breach**

- 1.71 Management reported the only major cyber incident that occurred during our audit period was the well-publicized cyberattack on the province's secure file transfer platform (MOVEit), that resulted in widespread theft of personal data
- 1.72 Our audit examined if the steps outlined in CSDS's Major Incident Management process were followed. Although our testing confirmed the Major Incident response process was applied during the MOVEit breach, internal documents following the breach showed lessons learned and proposed improvement to the plan.

### **Failure to Appropriately Manage Cybersecurity Risks by DHW, NSH and CSDS**

#### **Risk management is important for maintaining cybersecurity**

- 1.73 The NIST cybersecurity framework provides a risk-based approach to managing cybersecurity by implementing controls, processes, and strategies for risk management. Areas of activity and emphasis of the framework include managing third-party risks; managing configurations and systems throughout their life cycle; and protecting the confidentiality, integrity and availability of information.

#### **Widespread reliance on vendors to deliver digital health projects**

- 1.74 Management and internal documents establish Nova Scotia's digital health network relies on a wide range of vendors to provide different components of the technology that make up the network. Contracts with vendors or "third parties" are part of the supply chain for digital services and assets. Best practices are to use contracts to implement appropriate cybersecurity measures and routinely assess suppliers and third parties using audits, tests and other forms of evaluation to confirm they are meeting their contractual obligations.
- 1.75 CSDS created detailed cybersecurity recommendations for contracted vendors. The recommendations were intended to be attached to technology contracts. We examined the security recommendations and found they set out detailed controls and protections for the province's assets, including:
  - Maintain patching and updates,
  - Maintain anti-virus, anti-malware, and event detection and response,
  - Notify the province of any cybersecurity incidents,



- Maintain logging of activity within the asset,
- Control access and privileges, security controls, and boundary protection,
- Obtain, at least annually, penetration testing and vulnerability scanning,
- Obtain independent security assurance certifications.

### Health sector vendor IT contracts not required to include cybersecurity provisions

- 1.76 Management at DHW and CSDS told us that CSDS cybersecurity recommendations, discussed above, are not required for health technology projects, and their use is not enforced for the health sector. Management indicated even if the recommendations are used, they can be redacted or struck out at the vendor's request. Management at NSH expressed during our audit period that they were currently attempting to determine what security requirements should be included in vendor IT contracts.
- 1.77 NSH staff indicated a lack of consistent procurement and contracting requirements. We selected a sample of vendor agreements for further testing. Most contained minimal cybersecurity provisions. Without detailed contract provisions setting out vendor requirements, there is nothing to ensure cybersecurity performance in the vendor-controlled assets within the health system.

### Management of vendor IT contracts is still lacking, needs significant improvement

- 1.78 NSH and CSDS manage vendor IT contracts separately. Neither conduct regular compliance checks or follow-ups with vendors to confirm contract deliverables are met. Once a contract is signed, there are no processes in place to manage contracts, and compliance follow-up is rarely done.
- 1.79 During the 2019 audit of the province's Freedom of Information web portal, we found an over reliance on a vendor to ensure security, and contracts missing key components. We recommended that CSDS "establish a process to ensure and document vendor compliance with contract terms at all stages of a contract." Now more than five years later, we observed there are still no compliance checking processes to manage the technology contracts by either NSH or CSDS.
- 1.80 The considerable reliance on vendors to provide digital assets and services without adequate cybersecurity contract terms poses a significant risk to the cybersecurity of the digital health network. This issue is compounded by our observation that there is no review process to check if contracts are being fulfilled by vendors.

#### **Recommendation 1.13**

We recommend DHW, NSH and CSDS implement minimum cybersecurity contract provisions for all technology projects connecting to the digital health network.

#### **Health and Wellness, Nova Scotia Health and Cyber Security and Digital Solutions Response:**

The audit period also coincided with Nova Scotia's emergency response to the COVID-19 pandemic. The pandemic strained Nova Scotia's healthcare systems. To ensure the health and safety of all Nova Scotians, NSH altered care delivery systems in a rapid fashion including the emergency implementation of several key systems.

CSDS and DHW will continue to maintain a Security Obligations contract schedule that includes recommended cybersecurity provisions for technology projects. Delivery teams take a risk-based approach to tailor these provisions.

NSH has established standardized cyber contract schedules. Establishment of these schedules occurred outside the audit period. Target Date: Complete.

**Recommendation 1.14**

We recommend DHW, NSH and CSDS amend existing contracts to include the minimum cybersecurity contract provisions, or where not possible, take appropriate action to mitigate the impact of the missing provisions.

**Health and Wellness, Nova Scotia Health and Cyber Security and Digital Solutions Response:** NSH, DHW and CSDS are not able to impose additional security requirements on current contracts unilaterally. Vendors would need to agree to any change in terms.

Security requirements for existing contracts will be reviewed at the time of renewal or as new contracts are negotiated. Target Date: Ongoing.

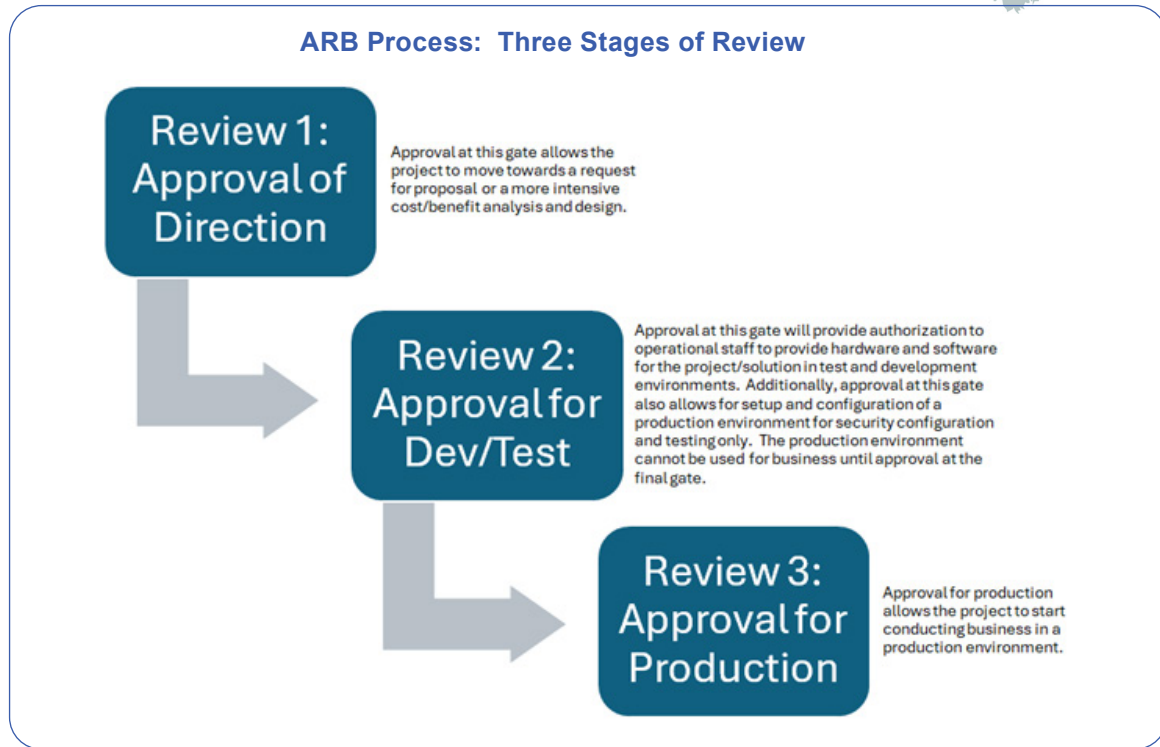
**Recommendation 1.15**

We recommend DHW, NSH and CSDS insist on vendor compliance with contract terms at all stages of a contract, including validating vendor compliance with the minimum cybersecurity provisions.

**Health and Wellness, Nova Scotia Health and Cyber Security and Digital Solutions Response:** DHW, NSH and CSDS will continue to work with vendors to ensure they meet minimum cyber security provisions. By December 2025, a formal process and related procedure will be established which is part of overall contract management processes. Target Date: December 2025.

 **Architecture Review Board to review and approve technology projects**

- 1.81 The function of the Architecture Review Board (ARB) is to review and approve proposed technology projects, focusing on alignment with policies and standards, including cybersecurity. The ARB includes experts from both CSDS and NSH with experience in areas such as Architecture, Cybersecurity and Information Management. All technology projects adding or changing existing architecture, data, or data flow on the digital health network are expected to go through the ARB process.
- 1.82 The ARB process includes three reviews at various stages by the ARB subject matter experts. Each review represents a check point for the experts to review the project and vote whether to move the project forward to full production. The ARB review relies on documentation being submitted to verify controls are in place prior to moving to the next stage in the review.
- 1.83 Although the ARB is composed of 15 disciplines, only three disciplines (cybersecurity, information privacy, and information services) are required to vote. It is up to the discretion of the other members (such as those from Foundational Digital Services, Supportive Digital Services and Health Services), to decide if the project relates to their field and if they will vote on the given project.



*\*As of May 2023, ARB Review Steps 2 & 3 have been consolidated  
Source: Office of the Auditor General of Nova Scotia*

### **Testing shows most projects do not fully comply with the ARB process**

- 1.84 Most of the projects we selected for testing did not comply fully with the process. We found common issues, such as missing approvals, no evidence of review, and missing documentation.

### **ARB pressured to rush projects**

- 1.85 CSDS staff told us there is pressure to review high priority projects quickly, even when doing so means not following the ARB process. With the added emphasis government has placed on “digitizing” the health network, there is an emphasis to fast track projects through the ARB process that can weaken the ARB as a control. CSDS personnel described projects that must be accomplished within a short time frame and gave an example of a project where staff were pushed by management to vote yes before cybersecurity risk assessments were completed to expedite the ARB process. We observed cybersecurity assessments were eventually completed for the project.
- 1.86 The business risk acceptance decision by the health business owner prevails in the ARB process. As described above, NSH’s current policy allows for this because NSH business owners can decide which standards are applied on a project-by-project basis. Without a commitment to enforce cybersecurity standards, the ARB is a weak mechanism for managing cybersecurity risks.

### **Projects tested did not meet cybersecurity standards after completing the ARB process**

- 1.87 We asked our cybersecurity expert to test the sample projects that had completed the ARB process against industry benchmarks and the established standards. This testing confirmed significant non-compliance with cybersecurity standards.

## ARB allows projects to connect to the digital health network without meeting cybersecurity standards

1.88 The ARB provides a control opportunity by vetting projects through experts, including cybersecurity, before connecting to the digital health network. However, the ARB process is not strictly followed. Voters are pressured to go quickly and vote yes. Business owners can accept identified cybersecurity risks. Our technical testing found the projects we tested which had completed the ARB process had significant noncompliance with cybersecurity standards. In our opinion, the ARB is not effectively managing cybersecurity risk in technology projects.

## ARB not effectively managing cybersecurity risk

1.89 Minimum standards for cybersecurity should be required for the digital health network. The digital health network processes a large and complex volume of patient data that is at risk if the network does not meet security standards. Overall, in our opinion, the ARB process provides a framework for accountability in managing what assets connect to the digital health network. However, the current process needs to be improved to effectively manage cybersecurity risk.

### **Recommendation 1.16**

We recommend DHW, NSH and CSDS adhere strictly to the ARB process and only allow projects to connect to the digital health network that have completed ARB and meet cybersecurity standards.

### **Health and Wellness, Nova Scotia Health and Cyber Security and Digital Solutions Response:**

The audit period also coincided with Nova Scotia's emergency response to the COVID-19 pandemic. The pandemic strained Nova Scotia's healthcare systems. To ensure the health and safety of all Nova Scotians, NSH altered care delivery systems in a rapid fashion including the emergency implementation of several key systems.

NSH has established procedures to ensure that all open cyber risks are addressed in a timely manner. Establishment of these procedures occurred outside the audit period.

CSDS, NSH and DHW will collaborate to define a digital assurance process to ensure solutions meet cybersecurity standards. Target Date: October 2025.

## Testing shows health decision makers frequently accept cybersecurity risks

1.90 As mentioned previously, in 2021 the IMIT Steering Committee stopped the use of Business Risk Acceptance Forms (BRAFF) which allowed business owners to decline all cybersecurity risk assessments for their technology projects. However, personnel also told us similar risk acceptance by business owners is still done. Business owners may accept cyber security risks informally via email or by using another risk acceptance form. The only difference is that business owners now complete the cybersecurity assessment before accepting risks. On the new forms, the business owner decides how they will treat identified risks by selecting accept, avoid, or mitigate.

1.91 Our testing focused on evaluating how business owners treated the identified risks in a sample of digital assets. Some of our sample digital assets had one identified cybersecurity risk, others had multiple risks identified. Some were connected to the digital health network already when the risk was identified, others had risks identified during project phases before connecting to the digital health network. The risk level assigned also varied, with some showing as critical or high and others showing as medium or low risk.

1.92 Management confirmed decisions on how to treat identified cybersecurity risks fall to the business owner and are done on an ad hoc basis. Individual business owners decide which cybersecurity standards to apply, and which risks to accept or mitigate.

1.93 For the sampled digital assets, our testing showed business owners frequently accepted cybersecurity risks.

### CSDS tracks some cybersecurity risks but do not use these to manage risks

1.94 CSDS has a risk register to track flagged cybersecurity risks, but they do not use it to follow-up with business owners about outstanding risks. Our audit found the resources associated with the follow-up function were moved elsewhere.

### Weaknesses in managing cybersecurity risk identified

1.95 We reviewed the auditees approach to managing risks on the cybersecurity network and identified many weaknesses in this area. Due to the sensitivity of the findings, details have not been publicly disclosed to protect the security of the digital health network. Our observations were supported by the results of our cybersecurity expert.

### Unaddressed risk persists in important clinical system

1.96 We noted an unaddressed risk remains in an important clinical system, demonstrating weakness in the risk management processes. Despite the risk being identified by an employee years ago, the issue has not been corrected. According to our cybersecurity expert, the risk is still active in the asset even after a system upgrade.



1.97 Without effective mechanisms of accountability to prompt and verify risk management and risk mitigation, known and unknown risks accumulate on the network, persisting despite best efforts.

#### **Recommendation 1.17**

We recommend DHW and NSH stop all ad hoc business risk acceptance practices and implement clear risk tolerance thresholds tied to cybersecurity standards and aligned with the custodian's responsibilities under the *Personal Health Information Act*.

**Health and Wellness and Nova Scotia Health Response:** CSDS, NSH and DHW will continue to take a holistic view of risk that balances the risk of urgent patient care and cyber security. The partners will work collectively to review existing processes for the management of cyber risks that fall outside defined risk tolerance thresholds. This work will align with evolving governance structures (recommendation 1.1). Target Date: October 2025.

#### **Recommendation 1.18**

We recommend DHW and NSH establish an accountability mechanism to verify planned risk mitigations are completed for all digital assets.

**Health and Wellness and Nova Scotia Health Response:** NSH has established procedures to ensure that open cyber risks for IT assets currently monitored by NSH are assessed, and where relevant, have planned mitigations. Establishment of these procedures occurred outside the audit period.

DHW will develop procedures to ensure cyber risks are assessed, and where relevant, are addressed in a timely manner. Target Date: June 2025.

### Ongoing risk management in digital assets is weak and unreliable

- 1.98 Digital assets require intentional, ongoing cyber security management to maintain standards and safety throughout the life cycle of the asset. For example, common risk management procedures can include prompts to change default passwords or apply security patches. These activities ensure risk management happens in a timely way and provide the basis for accountability mechanisms. A growing digital health network with complex interfaces requires significant planning and support to maintain.
- 1.99 The digital assets connected to Nova Scotia's digital health network are managed by several parties in complex arrangements. This was confirmed by management who indicated the arrangements for supporting digital assets vary by asset in a combination of support models, including support by CSDS; support by NSH; support by a vendor; or commonly, a combination of the three.

### Lack of clarity for roles and responsibilities weakens risk management

- 1.100 Managing cyber risks for a large and complex network needs clear roles and responsibilities, otherwise the environment is ripe for gaps and important actions to be missed. For example, the ongoing management of clinical applications is complex. Many clinical applications are used for a wide variety of functions across the healthcare system, often involving large amounts of patient data and complex technical structures of hardware, software, and databases.
- 1.101 Management confirmed the lack of role clarity persists. Employees told us about situations where lack of clear roles sometimes caused difficulties. We observed instances in interviews with CSDS, NSH and DHW where the lack of clarity in roles and responsibilities was evident by the inconsistencies in identifying responsibility for specific risk management activity.
- 1.102 The lack of role clarity for managing ongoing cybersecurity was observed during technical testing by our expert, and as a result, our experts were limited in their ability to complete controls testing.

### Lack of accountability mechanisms weakens risk management

- 1.103 Our inquiries about consistent standard operating procedures, checklists and other controls to manage expected cyber security risks in digital assets showed none in use and no formalized processes for managing ongoing cybersecurity in digital assets. Furthermore, our audit revealed CSDS staff, although responsible for critical risk management, have no authority to enforce key activities such as applying security patches and updates.

#### **Recommendation 1.19**

We recommend DHW, NSH and CSDS establish standard operating procedures with clear roles and responsibilities to provide for ongoing maintenance and management of cybersecurity risks in clinical medical devices, facilities and clinical applications.

**Health and Wellness, Nova Scotia Health and Cyber Security and Digital Solutions Response:** CSDS, NSH and DHW will review and enhance risk monitoring and reporting processes, clearly identify accountability for addressing risk and communication of asset risk to business owners for deployment of digital solutions including medical devices. Target Date: December 2025.





**Recommendation 1.20**

We recommend DHW, NSH and CSDS establish a mechanism to hold business owners accountable for maintaining security patches and updates in digital assets.

**Health and Wellness, Nova Scotia Health and Cyber Security and Digital Solutions Response:**

CSDS, NSH and DHW will review patch management processes and clearly identify accountability for maintaining security patches and updates in digital assets. Target Date: March 2025.

## Reasonable Assurance Engagement Description and Conclusions

We completed an independent assurance report of cybersecurity in health care at the Department of Health and Wellness, the Department of Cyber Security and Digital Solutions, and Nova Scotia Health. The purpose of this performance audit was to determine cybersecurity readiness in Nova Scotia's digital health network.

It is our role to independently express a conclusion about whether cybersecurity complies in all significant respects with the applicable criteria. Management at the Department of Health and Wellness, the Department of Cyber Security and Digital Solutions, and Nova Scotia Health have acknowledged their responsibility for cybersecurity in the digital health network.

This audit was performed to a reasonable level of assurance in accordance with the Canadian Standard on Assurance Engagements (CSAE) 3001 – Direct Engagements set out by the Chartered Professional Accountants of Canada; and sections 18 and 21 of the *Auditor General Act*.

We apply the Canadian Standard on Quality Management 1, which requires the Office to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

In conducting the audit work, we have complied with the independence and other ethical requirements of the Code of Professional Conduct of Chartered Professional Accountants of Nova Scotia as well as those outlined in Nova Scotia's Code of Conduct for public servants.

The objectives and criteria used in the audit are below:

**Objective:**

To determine the effectiveness of cybersecurity in Nova Scotia Health's digital networks.

**Criteria:**

1. The entities responsible for health system IT identify and control all hardware devices, software, network infrastructure and third parties that together make up the digital health networks.
2. The entities responsible for health system IT manage the security configurations for all hardware devices, software, network infrastructure and third parties to protect the digital health networks.
3. The entities responsible for health system IT continuously manage, control and report on all risks and vulnerabilities to protect the digital health networks.
4. The entities responsible for health system IT detect, respond to, and recover from cybersecurity threats and incidents demonstrating effective cybersecurity.

Generally accepted criteria consistent with the objectives of the audit did not exist. Audit criteria were developed specifically for this engagement. Criteria were accepted as appropriate by senior management at the Department of Health and Wellness, the Department of Cyber Security and Digital Solutions, and Nova Scotia Health.

Our audit approach consisted of interviews with management and staff of the Department of Health and Wellness, the Department of Cybersecurity and Digital Solutions, and Nova Scotia Health, reviewing policy, examining processes for cybersecurity and detailed file review. We examined relevant processes, plans, reports and other supporting documentation. Our cybersecurity technical expert conducted technical controls audit testing. Our audit period covered April 1, 2021 to June 1, 2023. We examined documentation outside of that period as necessary.

We believe the evidence we have obtained is sufficient and appropriate to provide the basis for our conclusions. Our report is dated October 21, 2024 in Halifax, Nova Scotia.

Based on the reasonable assurance procedures performed and evidence obtained we have formed the following conclusions:



Department of Health and Wellness, Nova Scotia Health, and Department of Cyber Security and Digital Solutions are not effectively providing cybersecurity for Nova Scotia's digital health networks.

- The entities responsible for health system IT do not effectively identify, control and manage all hardware devices, software, network infrastructure and third parties that together make up the digital health networks.
- The entities responsible for health system IT do not continuously manage, control and report on all risks and vulnerabilities to protect the digital health networks.
- The entities responsible for health system IT demonstrated some ability to respond and recover from cyber-attack but could improve the effectiveness by strengthening key network controls.

• • • Office of the Auditor General • • •

5161 George Street, Royal Centre, Suite 400

Halifax, Nova Scotia

B3J 1M7

[www.oag-ns.ca](http://www.oag-ns.ca)

[in/company/oag-ns](https://www.linkedin.com/company/oag-ns)

[X @OAG\\_NS](https://twitter.com/OAG_NS)

[f /OAGNS](https://www.facebook.com/OAGNS)

[@nsauditorgeneral](https://www.instagram.com/nsauditorgeneral)