

Chapter 3

Follow-up on Cybersecurity, Fraud Risk Management and Internal Meetings and Employee Social Events Expenses

Key Messages

- The Province and its organizations are still developing cybersecurity programs
- Government departments and organizations are still developing their responses to fraud risks

Why We Did This Chapter

- To provide updates on important matters impacting the Province

Cybersecurity

- Service Nova Scotia and Internal Services still has not finalized regulations which govern cybersecurity and its government-wide cybersecurity risk register is still under development
- Cybersecurity training programs are not provided to all IT users
- Organizations indicate they are moving forward in managing cybersecurity programs:
 - Housing Nova Scotia and Nova Scotia Municipal Finance Corporation indicated they have plans to discuss and determine their responsibilities regarding cybersecurity
 - Halifax-Dartmouth Bridge Commission indicated it addresses cybersecurity risks through its enterprise risk management program
 - Nova Scotia Health Authority indicated it began a review of cybersecurity

Fraud Risk Management

- Ten departments, nine public service units and 19 government organizations still have not completed fraud risk assessments
- Nine government organizations do not have fraud policies
- Atlantic Provinces Special Education Authority does not have a fraud policy, has not completed a fraud risk assessment, nor has it evaluated the usefulness of a fraud tip hotline
- Six departments and three public service units have fraud training completion rates below 80 per cent
- Not all departments and organizations evaluated and reported on their fraud risk management program in 2019-20



Questions Nova Scotians May Want to Ask

1. How prepared was the Province to respond to cybersecurity attacks during COVID-19?
2. What is the plan and timeline for finalizing the regulations under the Shared Services Act of 2014?
3. Does the Province plan to provide cybersecurity training for all IT users?
4. How will those organizations without a cybersecurity governance structure or risk management plan address their cybersecurity risks?
5. What is the Province's plan for departments and public service units to complete fraud risk assessments and when will they be done?

3 Follow-up on Cybersecurity, Fraud Risk Management and Internal Meetings and Employee Social Events Expenses

Purpose

- 3.1 The purpose of this chapter is to inform Nova Scotians on important matters impacting the Province. This year we followed up on cybersecurity, fraud risk management, and internal meetings and employee social events expenses.
- 3.2 To follow up on matters from our October 2019 Financial Report, we inquired of management at government departments, public service units, and organizations. The information we report in this chapter is not audited. We did not verify the accuracy of management's responses and do not provide assurance on management's comments. We did however confirm the contents of this chapter with the named organizations.
- 3.3 This survey work was conducted during COVID-19 and we wish to thank all those who responded to our survey questions during a challenging period.

Follow-up on Cybersecurity

- 3.4 Background – In 2019, we highlighted the status of the Province's and certain government organizations' cybersecurity risk management programs. We found there was a varied understanding of cybersecurity responsibilities.
- 3.5 Cybersecurity incidents can be caused by external hackers, business partners, vendors, contractors, or employees who either intentionally or unintentionally compromise cybersecurity. The Province is not immune to cybersecurity incidents and without proper cybersecurity measures, departments and organizations are at risk of the following threats:
 - data breaches
 - information held for ransom
 - theft of financial assets
 - misuse of personal or financial information
 - disruption of operations
- 3.6 COVID-19 further demonstrates the need for effective cybersecurity programs; cybersecurity experts report that due to the COVID-19 pandemic, threats from cyberattacks have grown in volume, scope, and severity. The



Canadian Centre for Cybersecurity reported that cyber criminals are quick to take advantage of high-profile events, particularly those that cause worry and concern, like a global pandemic.

- 3.7 The Canadian Centre for Cybersecurity has seen an increase in malicious attempts to access, damage, or attack networks that allow workers to work remotely. As with other jurisdictions, the global pandemic forced many provincial employees to work from home, further increasing the risks to the Province's cybersecurity with employees accessing the network from remote, non-government locations.
- 3.8 Also, in March 2020, the Canadian Centre for Cybersecurity issued an alert about the elevated risk faced by health organizations involved in the national response to COVID-19. It was reported that cyberattacks on the health sector have risen in 2019-20. Cybersecurity experts say the sector is targeted more than any other industry in the country; health information can be even more valuable to hackers than a credit card.

➡ Service Nova Scotia and Internal Services still has not finalized regulations which govern cybersecurity

- 3.9 In 2019, we reported that regulations under the Shared Services Act of 2014 were not yet finalized by the Department of Service Nova Scotia and Internal Services (SNS-IS). These regulations will outline what cybersecurity support services the Department will provide to which crown corporations, departments, and public sector entities.
- 3.10 SNS-IS management indicated that as of March 31, 2020, these regulations were not yet finalized because the realignment of the Department's operations required the draft regulations to undergo further revisions. SNS-IS also indicated it had been necessary to refocus the efforts and resources of the Department to respond to the impacts of COVID-19, thus further delaying finalization of the regulations. Finalizing the regulations will assist organizations in understanding their responsibilities for addressing cybersecurity risks.

➡ Service Nova Scotia and Internal Services' government-wide cybersecurity risk register is still under development

- 3.11 Last year we reported that the Province may not be managing all of its cybersecurity risks because its government-wide cybersecurity risk register was still in development through SNS-IS. At that time, the risk register only included cybersecurity risks identified and assessed on certain IT services delivered by SNS-IS; it was not government-wide.
- 3.12 During this year's follow-up, SNS-IS indicated it now has a process to assess cybersecurity risks for new IT projects and it plans to make major changes



to existing IT systems for all government departments and agencies. There remains a risk that older systems still in use throughout government have not been assessed. SNS-IS informed us that assessment of cybersecurity risks for these older systems will be considered in the future. To complete a government-wide cybersecurity risk register SNS-IS will need to close the gap by assessing cybersecurity risks associated with older systems still used throughout government.

➡ Cybersecurity training programs are not provided to all IT users

3.13 A key activity for managing cybersecurity risks is establishing processes for awareness and training. Providing cybersecurity awareness and training enhances the security environment and enables users to better understand their roles and responsibilities. Every user of the Province's network needs to understand the potential cyberthreats and the cybersecurity policies put in place to protect against those risks.

3.14 This year, when we asked SNS-IS management about the Department's training and awareness strategy for cybersecurity, it indicated it:

- shares information and educational materials with employees and partners which include government's information privacy groups and the health sector
- requires security assessments for IT projects and initiatives before they are approved
- established new cybersecurity obligations that are incorporated into new contracts with vendors

3.15 Although SNS-IS indicated it makes users aware of cybersecurity risks, it does not have a government-wide training program for all IT users. SNS-IS management said mandatory training on cybersecurity is limited to only some of its employees and those who process credit card transactions. Every user of the Province's network should understand their role and responsibilities.

➡ Organizations indicate they are moving forward in managing their cybersecurity programs

3.16 All government departments and organizations that own data, applications, servers, or manage networks have responsibilities and roles in relation to cybersecurity regardless of the services received from SNS-IS or other IT service providers.

3.17 In 2019, we surveyed financially significant government organizations in the area of cybersecurity and reported that some did not have a cybersecurity governance structure in place and/or had not implemented a cybersecurity



risk management program as of March 31, 2019. In 2020, management of the following three organizations indicated they are moving forward in managing their cybersecurity risks.

- Halifax-Dartmouth Bridge Commission – The Commission advised us that while they don't have a cybersecurity risk management program, they have components of a program and address cybersecurity risks through their enterprise risk management review program.
- Housing Nova Scotia – The Department of Municipal Affairs and Housing indicated that Housing Nova Scotia employees became part of the Department in 2019 and therefore follow the provincial processes and practices for a shared IT environment. The Department said it was working towards developing a shared model approach which will include Housing Nova Scotia and its housing authorities and is expecting to follow the risk management program for cybersecurity risks for the Province.
- Nova Scotia Municipal Finance Corporation – Management indicated it follows provincial policies and practices and was attempting to initiate discussions with Service Nova Scotia and Internal Services to discuss cybersecurity governance and risk management specific to the Corporation.

3.18 Also in 2019, we reported that the Nova Scotia Health Authority did not have a cybersecurity governance structure in place. We reported the Authority relied on Service Nova Scotia and Internal Services to manage its cybersecurity risks. We also indicated that SNS-IS's risk frameworks did not take into consideration the Nova Scotia Health Authority's clinical data and applications.

3.19 This year, management of the Nova Scotia Health Authority indicated it began a review of cybersecurity to identify requirements that will support a cybersecurity risk management program at the Authority that will align with the Province's cybersecurity program.

Follow-up on Fraud Risk Management

3.20 Background – Fraud within the public sector is concerning because it can result in the loss of taxpayer assets and reduce the public's confidence in the government and its ability to safeguard assets. Therefore, it is important for the Province to have mechanisms in place to appropriately manage fraud risks.

3.21 To assist in managing fraud risks, in 2017 the Province implemented a fraud policy. The policy directly applies to all government departments, public service units, and crown corporations, and although not required, it was



recommended that other government organizations embrace the intent of the policy. Government's Fraud Risk Management Program is governed by a Fraud Risk Management Committee, with representation from a cross section of government departments and the Public Service Commission, and oversight from the Deputy Ministers' Audit Committee. Specific components of the program include:

- fraud policies and procedures
- fraud risk assessments
- fraud awareness and education
- fraud prevention and detection techniques
- well-documented framework for reporting and investigating allegations of fraud

➔ Improvements still required in fraud risk management programs in government

3.22 We followed up with government departments, public service units, and organizations on the status of certain aspects of their fraud risk management programs. The table below summarizes the status as of March 31, 2020. Appendices I, II, and III show the status of each individual department, public service unit, and organization.

Summary Status of Certain Aspects of a Fraud Risk Management Program	
March 31, 2020	
Government Departments	
Fraud risk assessment completed	7 Yes (41%) 10 No (59%)
Public Service Units	
Fraud risk assessment completed	8 Yes (47%) 9 No (53%)
Government Organizations	
Fraud policy implemented	42 Yes (82%) 9 No (18%)
Fraud risk assessment completed	32 Yes (63%) 19 No (37%)
Usefulness of fraud hotline evaluated	45 Yes (88%) 6 No (12%)

➔ Ten departments and nine public service units still have not completed a fraud risk assessment

3.23 Fraud risk assessment – The following 10 departments (59%) told us they had not completed a fraud risk assessment as of March 31, 2020.



Departments That Have Not Completed a Fraud Risk Assessment as of March 31, 2020	
Agriculture	Fisheries and Aquaculture
Communities, Culture and Heritage	Lands and Forestry
Education and Early Childhood Development	Municipal Affairs and Housing
Energy and Mines	Seniors
Environment	Service Nova Scotia and Internal Services

3.24 See Appendix V for the Chair’s 2020 update on fraud risk assessments and other aspects of Government’s Fraud Risk Management Program.

3.25 This year we surveyed the Province’s public service units (PSUs) to determine which PSUs completed fraud risk assessments. Management from the following nine PSUs (53%) told us their organization had not completed a fraud risk assessment as of March 31, 2020.

Public Service Units That Have Not Completed a Fraud Risk Assessment as of March 31, 2020	
Aboriginal Affairs	Office of Immigration
Elections Nova Scotia	Office of Regulatory Affairs and Service Effectiveness
Freedom of Information and Protection of Privacy Review Office	Office of Ombudsman
Human Rights Commission	Public Service Commission
Nova Scotia Police Complaints Commissioner	



Nineteen government organizations still have not completed a fraud risk assessment

3.26 The following 19 organizations told us they had not completed a fraud risk assessment as of March 31, 2020.

Government Organizations That Have Not Completed a Fraud Risk Assessment as of March 31, 2020	
Annapolis Valley Regional Centre for Education	Nova Scotia Farm Loan Board
Art Gallery of Nova Scotia	Nova Scotia Fisheries and Aquaculture Loan Board
Arts Nova Scotia	Nova Scotia Health Authority
Atlantic Provinces Special Education Authority	Nova Scotia Legal Aid Commission
Canadian Sports Centre Atlantic	Nova Scotia Primary Forest Products Marketing Board
Cape Breton-Victoria Regional Centre for Education	Nova Scotia Strategic Opportunities Fund Incorporated
Chignecto-Central Regional Centre for Education	Perennia Food & Agriculture Incorporated
Creative Nova Scotia Leadership Council	South Shore Regional Centre for Education



Government Organizations That Have Not Completed a Fraud Risk Assessment as of March 31, 2020 (Continued)	
Halifax Convention Centre Corporation	Tri-County Regional Centre for Education
Halifax Regional Centre for Education	

➔ Nine government organizations do not have a fraud policy

3.27 Fraud policy – Management of the following nine government organizations told us they had not implemented a fraud policy before March 31, 2020.

Government Organizations That Have Not Implemented a Fraud Policy as of March 31, 2020	
Annapolis Valley Regional Centre for Education	Nova Scotia Primary Forest Products Marketing Board
Atlantic Provinces Special Education Authority	South Shore Regional Centre for Education
Cape Breton-Victoria Regional Centre for Education	Strait Regional Centre for Education
Chignecto-Central Regional Centre for Education	Tri-County Regional Centre for Education
Conseil scolaire acadien provincial	

3.28 Last year, the Department of Education and Early Childhood Development noted it would implement a common fraud policy for all Regional Centres for Education and Conseil scolaire acadien provincial. However, the Department indicated that due to COVID-19, they were not able to implement the policy before March 31, 2020.

➔ Government organizations still have not evaluated the usefulness of a fraud tip hotline

3.29 Fraud tip hotline – Research shows that tips are the most common method of detecting fraud. In 2017 we first reported that no government department had a fraud tip hotline. The Province has since evaluated the usefulness of a fraud tip hotline and launched a fraud reporting service in November 2020 for government departments and certain public service unit employees.

3.30 Government organizations should also evaluate the usefulness of a fraud tip hotline. As of March 31, 2020, the following six government organizations indicated they had not evaluated the usefulness of a fraud tip hotline.

Government Organizations That Have Not Evaluated the Usefulness of a Fraud Tip Hotline as of March 31, 2020	
Atlantic Provinces Special Education Authority	Nova Scotia School Insurance Exchange
Canadian Sports Centre Atlantic	Nova Scotia School Insurance Program Association
Nova Scotia Primary Forest Products Marketing Board	Public Archives of Nova Scotia



➔ Atlantic Provinces Special Education Authority does not have a fraud policy, a fraud risk assessment, and has not evaluated the usefulness of a fraud hotline

3.31 As can be seen in the tables above, Atlantic Provinces Special Education Authority (APSEA) does not have a fraud policy, has not completed a fraud risk assessment, and has not evaluated the usefulness of a fraud hotline. APSEA is an inter-provincial organization with assets of over \$32 million and annual revenues that exceed \$18 million. It should have a fraud risk management program.

➔ Six departments and three public service units have fraud training completion rates below 80%

3.32 Fraud training – Following implementation of Government’s Fraud Policy in June 2017, fraud training became available and mandatory for employees of government departments and public service units.

3.33 The table below shows the six government departments and three public service units that reported fraud training completion rates below 80 per cent as of March 31, 2020. Appendices I and II show the reported fraud training completion rates of each individual department and public service unit.

Government Departments and Public Service Units with a Fraud Training Completion Rate Below 80% as of March 31, 2020	
	% of Employees who Completed Fraud Training
Government Department	
Community Services	54%
Lands and Forestry	61%
Transportation and Infrastructure Renewal	65%
Agriculture	67%
Fisheries and Aquaculture	69%
Energy and Mines	72%
Public Service Unit	
Public Prosecution Service	60%
Human Rights Commission	75%
Nova Scotia Securities Commission	75%

3.34 It is very important that departments and public service units have all their employees complete the mandatory fraud training. Low completion rates of mandatory fraud training diminish the Province’s ability to effectively manage fraud.



➔ Not all government departments and organizations evaluated and reported on their fraud risk management program in 2019-20

3.35 Regularly evaluating and reporting on fraud risk management operations helps a department or organization ensure it has designed an appropriate process that prevents and detects fraud in the current environment. Therefore, government departments and organizations should regularly evaluate and report on how well they are managing fraud risks.

3.36 In 2020 we followed up with departments and financially significant government organizations to see if they had evaluated and reported on their fraud risk management programs in 2019-20. The table below summarizes the responses. Appendices I and IV show the response of each individual department and organization.

Summary of Evaluating and Reporting on Fraud Risk Management Programs at Government Departments and Significant Organizations in 2019-20	
	Evaluated and Reported
Government Departments	6 Yes (35%) 11 No (65%)
Government Organizations	6 Yes (55%) 5 No (45%)

Follow-up on Internal Meetings and Employee Social Events Expenses

3.37 In 2018, we examined internal meetings and employee social events costs to determine if these expenses complied with existing policies, were appropriately supported, and correctly classified. From this work in 2018, we noted a lack of formalized policy across government in the areas of internal meetings and employee social events. We recommended that Executive Council provide guidance on internal meetings and employee social event expenses that clarified the nature and accounting of acceptable costs to ensure these expenses meet public expectations, are supportable, and well-documented.

3.38 As part of last year’s follow-up for 2019, Executive Council informed us that discussions were ongoing and the goal was to implement corporate guidelines by January 1, 2020. Our follow-up with Executive Council in 2020 revealed that they updated, by January 1, 2020, the Province’s Discretionary Spending Policy to include Guidelines for Meeting and Related Expenses.



Appendix I

Management's Responses from Government Departments Regarding Certain Aspects of a Fraud Risk Management Program as of March 31, 2020

Government Department	Fraud Risk Assessment	Evaluate and Report on Fraud Risk Management Process	% of Employees who Completed Fraud Training
Agriculture	No*	No	67%
Business	Yes	No	92%
Communities, Culture and Heritage	No*	No	100%
Community Services	Yes	No	54%
Education and Early Childhood Development	No	No	81%
Energy and Mines	No	No	72%
Environment	No*	No	94%
Finance and Treasury Board	Yes	Yes	88%
Fisheries and Aquaculture	No*	No	69%
Health and Wellness	Yes	No	80%
Justice	Yes	Yes	83%
Labour and Advanced Education	Yes	Yes	90%
Lands and Forestry	No*	No	61%
Municipal Affairs and Housing	No*	Yes	94%
Seniors	No	No	100%
Service Nova Scotia and Internal Services	No*	Yes	83%
Transportation and Infrastructure Renewal	Yes	Yes	65%
Total	7 Yes (41%) 10 No (59%)	6 Yes (35%) 11 No (65%)	-

* Management indicated progress is being made



Appendix II

Management's Responses from Public Service Units Regarding Certain Aspects of a Fraud Risk Management Program as of March 31, 2020

Public Service Unit	Fraud Risk Assessment	% of Employees who Completed Fraud Training
Aboriginal Affairs	No*	100%
Communications Nova Scotia	Yes	97%
Elections Nova Scotia	No	93%
Executive Council	Yes	100%
Freedom of Information and Protection of Privacy Review Office	No	100%
Human Rights Commission	No	75%
Intergovernmental Affairs	Yes	94%
Legislative Services	Yes	94%
Nova Scotia Police Complaints Commissioner	No	100%
Nova Scotia Securities Commission**	Yes	75%
Office of Immigration	No	92%
Office of Regulatory Affairs and Service Effectiveness	No	100%
Office of Strategy Management	Yes	100%
Office of the Auditor General	Yes	100%
Office of the Ombudsman	No	100%
Public Prosecution Service**	Yes	60%
Public Service Commission	No	91%
Total	8 Yes (47%) 9 No (53%)	-

* Management indicated progress is being made

** Nova Scotia Securities Commission and Public Prosecution Service have not completed fraud risk assessments specific to their public service unit; the risks in those units have been considered within the fraud risk assessment of the Department of Finance and Treasury Board. The fraud risk assessment response provided here is the response of the Department of Finance and Treasury Board.



Appendix III

Management's Responses from Government Organizations Regarding Certain Aspects of a Fraud Risk Management Program as of March 31, 2020

Government Organization	Fraud Policy	Fraud Risk Assessment	Evaluated Usefulness of Fraud Hotline
A. Education Sector			
Annapolis Valley Regional Centre for Education	No*	No*	Yes
Atlantic Provinces Special Education Authority	No	No	No
Cape Breton-Victoria Regional Centre for Education	No*	No*	Yes
Chignecto-Central Regional Centre for Education	No*	No*	Yes
Conseil scolaire acadien provincial	No*	Yes	Yes
Halifax Regional Centre for Education	Yes	No*	Yes
Nova Scotia Community College	Yes	Yes	Yes
Nova Scotia Education Common Services Bureau	Yes	Yes	Yes
Nova Scotia School Insurance Exchange	Yes	Yes	No
Nova Scotia School Insurance Program Association	Yes	Yes	No
South Shore Regional Centre for Education	No*	No*	Yes
Strait Regional Centre for Education	No*	Yes	Yes
Tri-County Regional Centre for Education	No*	No*	Yes

B. Health Sector			
Izaak Walton Killam Health Centre	Yes	Yes	Yes
Nova Scotia Health Authority	Yes	No*	Yes

C. Sizeable Organizations			
Art Gallery of Nova Scotia	Yes	No	Yes
Canada-Nova Scotia Offshore Petroleum Board	Yes	Yes	Yes
Develop Nova Scotia	Yes	Yes	Yes
Halifax Convention Centre Corporation	Yes	No	Yes
Halifax-Dartmouth Bridge Commission	Yes	Yes	Yes
Harbourside Commercial Park Inc.	Yes	Yes	Yes
Highway 104 Western Alignment Corporation	Yes	Yes	Yes
Housing Nova Scotia	Yes	Yes	Yes
Nova Scotia Business Inc.	Yes	Yes	Yes
Nova Scotia Crop and Livestock Insurance Commission	Yes	Yes	Yes
Nova Scotia Farm Loan Board	Yes	No	Yes
Nova Scotia Fisheries and Aquaculture Loan Board	Yes	No	Yes
Nova Scotia Gaming Corporation	Yes	Yes	Yes



Management's Responses from Government Organizations Regarding Certain Aspects of a Fraud Risk Management Program (Continued)

Government Organization	Fraud Policy	Fraud Risk Assessment	Evaluated Usefulness of Fraud Hotline
C. Sizeable Organizations			
Nova Scotia Innovation Corporation	Yes	Yes	Yes
Nova Scotia Lands Inc.	Yes	Yes	Yes
Nova Scotia Legal Aid Commission	Yes	No	Yes
Nova Scotia Liquor Corporation	Yes	Yes	Yes
Nova Scotia Municipal Finance Corporation	Yes	Yes	Yes
Nova Scotia Power Finance Corporation	Yes	Yes	Yes
Nova Scotia Utility and Review Board	Yes	Yes	Yes
Public Archives of Nova Scotia	Yes	Yes	No
Tourism Nova Scotia	Yes	Yes	Yes
D. Others			
Arts Nova Scotia**	Yes	No*	Yes
Canadian Sports Centre Atlantic	Yes	No	No
Council of Atlantic Premiers	Yes	Yes	Yes
Creative Nova Scotia Leadership Council**	Yes	No*	Yes
Gambling Awareness Foundation of Nova Scotia	Yes	Yes	Yes
Invest Nova Scotia Board	Yes	Yes	Yes
Nova Scotia Primary Forest Products Marketing Board***	No	No	No
Nova Scotia Strategic Opportunities Fund Incorporated****	Yes	No	Yes
Perennia Food & Agriculture Incorporated	Yes	No	Yes
Resource Recovery Fund Board Inc.	Yes	Yes	Yes
Schooner Bluenose Foundation	Yes	Yes	Yes
Sherbrooke Restoration Commission	Yes	Yes	Yes
Sydney Steel Corporation	Yes	Yes	Yes
Sydney Utilities Limited	Yes	Yes	Yes
Total	42 Yes (82%) 9 No (18%)	32 Yes (63%) 19 No (37%)	45 Yes (88%) 6 No (12%)

* Management indicated progress is being made

** Arts Nova Scotia and Creative Nova Scotia Leadership Council have not completed fraud risk assessments specific to their organization; the risks in those units have been considered within the fraud risk assessment of the Department of Communities, Culture and Heritage. The fraud risk assessment response provided here is the response of the Department of Communities, Culture and Heritage.

*** Nova Scotia Primary Forest Products Marketing Board has not implemented a fraud policy, completed a fraud risk assessment or evaluated the usefulness of a fraud tip hotline. The Board has been inactive with no Board appointees or staff since February 26, 2018.

**** Nova Scotia Strategic Opportunities Fund Incorporated has not completed a fraud risk assessment as there are no staff and there is no activity. The Fund is being wound down with the final few transactions administered by the Department of Finance and Treasury Board.



Appendix IV

Management's Responses from 11 of the Province's Financially Significant Organizations Regarding Evaluating and Reporting on the Effectiveness of Their Fraud Risk Management Program in 2019-20

Government Organization	Evaluate and Report on Effectiveness of Fraud Risk Management
Develop Nova Scotia	Yes
Halifax-Dartmouth Bridge Commission	Yes
Halifax Regional Centre for Education	No
Housing Nova Scotia	No
Izaak Walton Killam Health Centre	Yes
Nova Scotia Community College	Yes
Nova Scotia Farm Loan Board	No
Nova Scotia Health Authority	Yes
Nova Scotia Legal Aid Commission	No
Nova Scotia Liquor Corporation	No
Nova Scotia Municipal Finance Corporation	Yes
Total	6 Yes (55%) 5 No (45%)



Appendix V

Update from the Chair of the Deputy Minister's Audit Committee on Government's Fraud Risk Management Program

The Deputy Ministers' Audit Committee oversees the Province of Nova Scotia's Fraud Risk Management Program. The comprehensive Program includes a fraud governance structure, fraud policy and reporting procedures, fraud training and awareness, fraud risk assessments, fraud investigations, third party fraud reporting services (i.e. fraud tip hotline) and continuous improvement activities, applicable to Government departments and some public service units. Fraud risk management activities related to other public service units and Government organizations noted within the results of this report are not within the scope of their authority. The following response is related to activities within the Deputy Ministers' Audit Committee scope of responsibility.

Government departments and certain public service units have a Fraud Risk Management Program to prevent, deter and detect fraud, including managing the risk of fraud. The Program is governed by a Fraud Risk Management Committee, with representation from a cross section of government departments and the Public Service Commission, and oversight from the Deputy Ministers' Audit Committee. A formal Mandate for the Fraud Risk Management Committee outlines its purpose, authority, responsibilities and composition. The step-by-step implementation of this Program is an explicit demonstration of Government's commitment to a strong ethical workforce and a sustainable culture of respect, integrity, diversity, accountability and the public good.

A Fraud Policy was included in Management Manual 200 in 2017 and is reviewed and updated annually as required. The Policy is supported by detailed procedures for reporting and investigating fraud. In addition, mandatory fraud awareness training has been available online for government employees since the Policy was released. This has been completed by more than 9,567 employees as of July 2020.

Government departments and certain public service units are committed to the completion of fraud risk assessments to identify and assess the likelihood and significance of specific fraud schemes and risks, evaluate control activities, and implement action to address fraud risks. Fraud risk assessments are completed and in progress; however, the completion rates need to improve. Government is supporting this effort with the use of a fraud risk assessment framework to ensure assessments meet an appropriate standard and are consistently applied; a fraud risk self-assessment toolkit distributed to the departments to assess and identify areas at a high risk for fraud; a streamlined process for procuring fraud risk assessments from a third party service provider; and an experienced team of fraud investigators with experience completing fraud risk assessments.

An independent third-party vendor manages the Provincial Fraud Reporting Service (e.g. hotline, webform, email reporting). The reporting service is available to Government departments and certain public service unit employees 24 hours a day, 365 days per year. This reporting service was launched in November 2020.