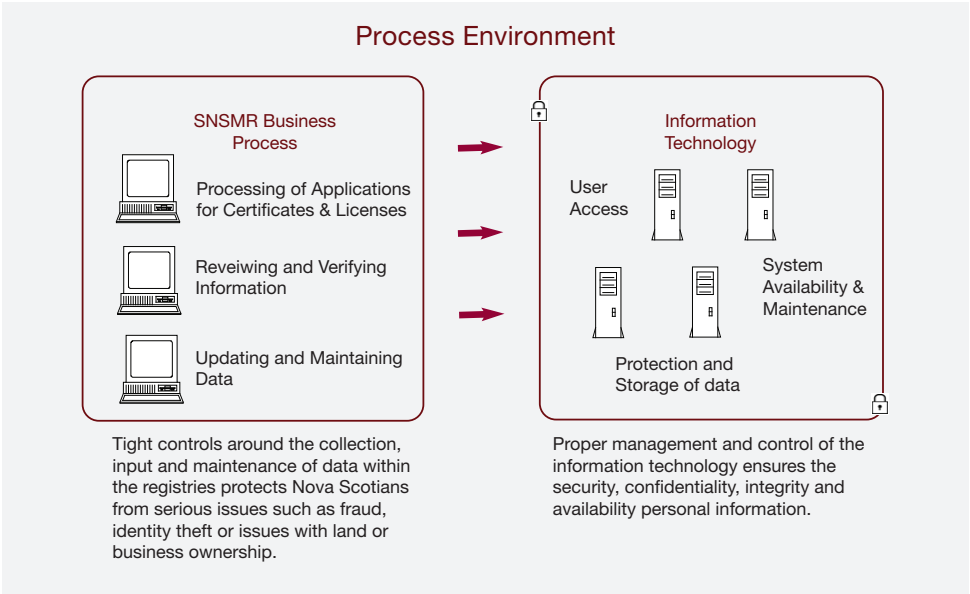
4 Service Nova Scotia and Municipal Relations: Registry Systems

Summary

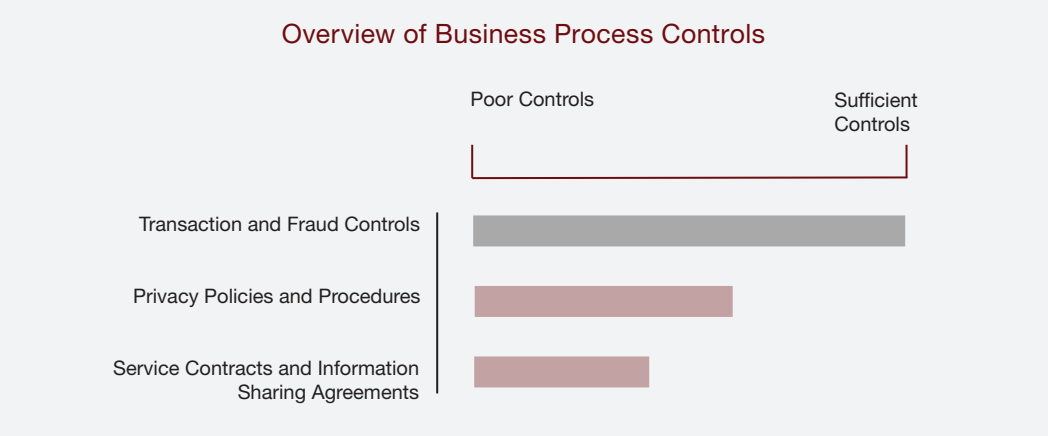
The Department of Service Nova Scotia and Municipal Relations (SNSMR) does not have adequate controls in place to ensure the confidentiality, integrity and availability of information in certain of its registries. Strong control is required to protect the privacy, safety and economic viability of the Department's public and business clients.

SNSMR is responsible for issuing the majority of the provincial government's licenses, permits, registrations and certificates. Many important business and personal activities cannot proceed without these documents. Collection of a significant amount of information from individuals and businesses is necessary to assess their eligibility. Much of this information is inherently sensitive and needs adequate levels of security and control to protect its confidentiality, integrity and continued availability. Business units within SNSMR administer these processes through registries, including the four that were the subject of our audit: Land Registry, Registry of Joint Stock Companies, Nova Scotia Business Registry, and Registry of Vital Statistics.

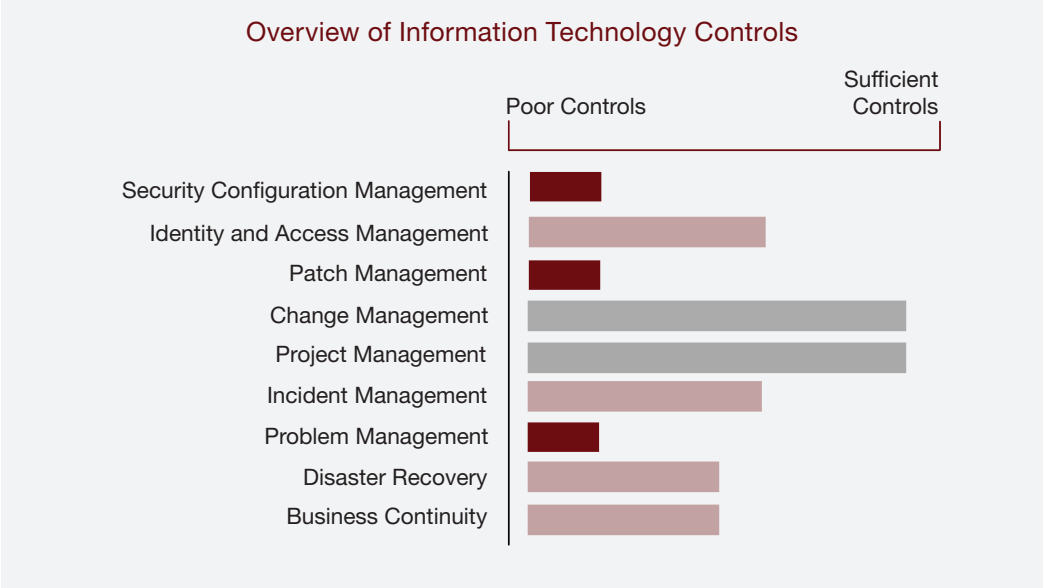
To process licenses, permits, registrations and certificates, these business units rely heavily on departmental business processes, as well as the information technology (IT) functions that store and protect registry information. Both of these areas need to be well controlled and, consequently, were included in our audit.



Business Process Controls: We found the transaction processing controls associated with the registries were adequate. However, we identified shortcomings related to adequacy of communications; application and availability of privacy policies; and sufficiency of controls around service contracts. The following chart provides an overview of the state of the business process controls our audit tested.



Information Technology Controls: We concluded that there are security vulnerabilities stemming from weaknesses in areas such as security configuration settings, patch management and problem management. The following chart provides an overview of the state of the information technology controls our audit examined.



Our audit considered various methods to disrupt, corrupt or gain unauthorized access to the registries. We concluded that there is a risk of exploitation from system users operating within the provincial network, such as employees and contract staff. It

is important to note that internal threats can be equally as concerning as external threats. There have been at least two alleged cases of fraud by government employees reported in recent years. External hackers can also target internal contacts to exploit systems, through collusion, bribery and blackmail.

Unauthorized access to the systems or databases supporting the registries could result in the disclosure of sensitive information, modification or deletion of registry information, or disruption of registry operations. Impacts to individuals could include identity theft, loss of land ownership, inability to obtain needed information and certificates, or disruption of business operations.

The majority of our recommendations require relatively minimal resources to implement. These recommendations do not require the acquisition of new systems or expensive software, but rather configuration changes to existing systems and possibly additional policies and procedures. Furthermore, the control improvements we recommend will strengthen areas beyond the four registries we audited because other functions of the Department rely on the IT systems we examined.

4 Service Nova Scotia and Municipal Relations: Registry Systems

Background

4.1 The Government of Nova Scotia is responsible for information it collects on Nova Scotians, as well as thousands of businesses within the Province. For example, anyone who experiences a significant life event in Nova Scotia (e.g., birth, marriage, death), buys or sells land, or incorporates and operates a business in Nova Scotia must provide information to the provincial government.

4.2 The Department of Service Nova Scotia and Municipal Relations (SNSMR) maintains most of the government registries that issue licenses, permits, registrations and certificates to Nova Scotia businesses and members of the public. It maintains computer databases to support the various registries and, accordingly, relies heavily on information technology (IT). The four registries that were the subject of our audit are:

- *Nova Scotia Business Registry* – This registry enables the use of the Canada Revenue Agency's business number as the unique identifier for business clients. Through the use of the business number, this registry provides business licensing, permitting, registration and inspection services on behalf of SNSMR and other provincial government departments. The Nova Scotia Business Registry was formed through a partnership among SNSMR, the Canada Revenue Agency and the Workers' Compensation Board.

- *Registry of Joint Stock Companies* – This registry enables the formation and registration of various forms of business and non-profit organizations operating in Nova Scotia (e.g., companies, partnerships, sole-proprietorships and societies). This registry also provides the public with access to public information about these organizations.

- *Registry of Vital Statistics* – This registry maintains a record of all vital events that occur within the Province of Nova Scotia. This includes the registration of births, marriages, deaths, stillbirths and domestic partnerships, as well as issuing certificates relating to these events.

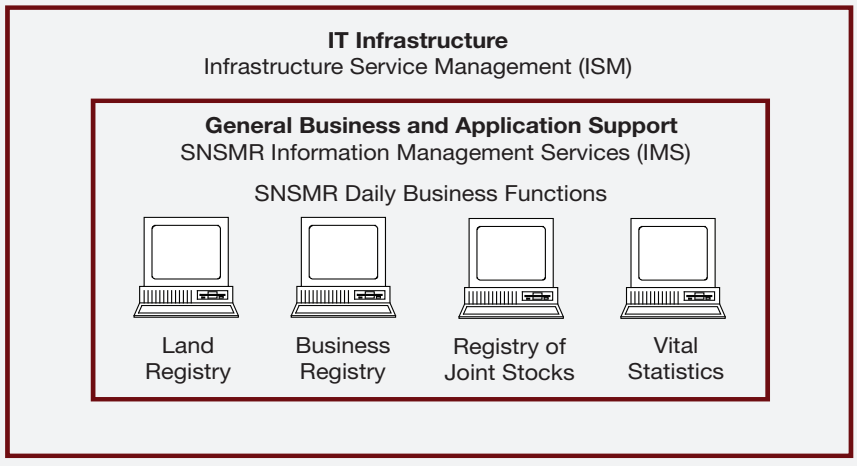
- *Land Registry* – This registry provides for the submission, processing and safe keeping of all real property transactions and related documents. It also creates and maintains a link between land interests and land parcel identifiers; and between the identifiers and the assessment accounts. Additionally, it provides appropriate access to land-related documents and information.

4.3 These four registries provide a central, electronic repository of information that is accessible to all authorized users, where there is access to government networks regardless of geographic location. Much of the information collected for these registries is inherently sensitive. Proper management of the information technology supporting these registries is critical to ensuring the confidentiality, integrity and availability of the information maintained in them. As well, strong controls will protect the public from negative experiences such as fraud, identity theft or inaccurate land and business ownership caused by inappropriate access to, and use of, the registries.

4.4 Groups within and outside the Department provide support for SNSMR's IT systems and daily business functions.

- *Information Management Services (IMS)* – This division of SNSMR is the primary group that manages the information technology that supports the various registries. IMS provides support for IT systems as well as some of the server support.
- *Infrastructure Service Management (ISM)* – This division of the Chief Information Office administers access to the wide-area network and manages IT infrastructure, including some of the servers that support the SNSMR registries. The servers are hosted at the provincial datacentre, which has recently become the responsibility of the Chief Information Office. At the time of our fieldwork, the Department of Community Services provided desktop support functions for hardware and access to the network. This responsibility has since been transferred to the Chief Information Office.

Support Environment



Audit Objectives and Scope

4.5 In the summer of 2010, we completed an audit of the IT infrastructure and service delivery processes supporting various registries at Service Nova Scotia and Municipal Relations (SNSMR). The engagement was conducted in accordance with Section 8 of the Auditor General Act and auditing standards established by the Canadian Institute of Chartered Accountants. The purpose of our audit was to determine if there are sufficient controls in place for the registries at SNSMR to adequately serve and protect businesses and members of the public who rely upon them. Audit fieldwork was conducted between September 2009 and April 2010, with a testing period covering transactions between September 1, 2008 and September 30, 2009.

4.6 The objectives of our audit were to assess the adequacy of:

- business controls and IT controls to ensure the completeness, accuracy and availability of information collected, produced and reported;
- fraud prevention practices, policies and procedures;
- systems and processes to protect the privacy of information collected and stored;
- procedures and policies to ensure the confidentiality, integrity and availability of web-based (e-commerce) information technology services; and
- control over information shared with other government entities.

4.7 We selected four registries to be the subjects of our audit: the Land Registry, Nova Scotia Business Registry, Registry of Joint Stock Companies and the Registry of Vital Statistics. We are not providing assurance on these registries individually. The findings from our examination of each support our opinion on the Department's overall management and control of these registries combined. We did not audit the controls around access to the systems from outside the Province's wide-area network. Management engaged an external firm to perform a vulnerability assessment that would look at these controls. This assessment was not finalized when we completed our audit.

4.8 We used criteria developed by our Office to audit the business processes of the four registries. The majority of the criteria used for assessing the registries' IT controls were taken from the IT Governance Institute's *Control Objectives for Information and related Technology (COBIT 4.1)*,

which is a widely-accepted international source of best practices for the governance, control, management and audit of IT operations. SNSMR also stores and processes credit card information and, as a result, is required to be compliant with the Payment Card Industry Data Security Standard (PCI DSS). Our audit approach, therefore, integrated the PCI DSS standard with COBIT standards.

4.9 These objectives and criteria were discussed with, and accepted as appropriate by, members of management responsible for the systems we audited.

Significant Audit Observations

Transaction and Fraud Controls

Conclusions and summary of observations

Controls around transaction processing are adequate, and particularly strong with respect to the Registry of Vital Statistics. However, we noted a lack of formalized procedures regarding management review and oversight of information maintained by the registries we audited. Strong control over day-to-day processing of transactions, as well as management's monitoring of these activities, are critical to preventing fraudulent activity and maintaining the completeness and accuracy of information in the registries.

4.10 *Transaction processing controls* – We examined a sample of business transactions from the period of September 1, 2008 to September 30, 2009 to determine compliance with departmental policies, procedures and related controls. No exceptions were identified during this testing period and, in particular, the controls in place within Vital Statistics to process, balance and manage information were found to be ideal. Vital Statistics employs a combination of manual and system controls to tightly manage and monitor information flow.

4.11 *Personally identifiable information* – It is policy of the Business Registry and the Registry of Joint Stock Companies to remove some personal information, such as credit card and social insurance numbers, from documentation retained. For documents under the central control of the business registries, we observed that staff members consistently remove specific personal information prior to scanning documents into the registry systems and when preparing them for filing. However, we observed several instances where documentation relating to licenses and permits maintained by government departments other than SNSMR still contained personal

information. This documentation is not available to the public, but increases the risk of inappropriate access.

4.12 *Fraud awareness* – Only the Vital Statistics business unit provides orientation and manuals that include a focus on fraud awareness. We suggested to the Department that the other registries might benefit from a strategy for providing effective fraud awareness, protection and detection training.

4.13 *Management reporting and monitoring* – There is a lack of formal management monitoring and review of transaction processing and data accuracy within three of the four registries we examined. More specifically, we found the following.

- The Land Registry has a process whereby supervisors are to regularly review transactions on a test basis to check the quality of staff members' work against policies and procedures. We found that this review had not been performed in four months.
- Staff of the Land Registry and the Registry of Joint Stock Companies review client applications with the aid of checklists to validate that client applications meet all requirements. There is no requirement to retain these checklists and therefore they are not available for review by management.
- Supervisors within the Business Registry have access to reports they can use to review the accuracy of transactions processed and to assess the productivity of staff. We could not determine whether this control procedure is operating properly because there is no evidence of this review.
- Section 2.1.3 IV of the Land Registration Act Agreement between the Department and the Barristers' Society of Nova Scotia requires the Department to perform *"...internal system quality control functions, by evaluating whether human and information technology resources of government are performing as expected."* During testing in November 2009, we noted this review had not been performed since March 2008.

4.14 It is important to verify that processed transactions are accurate and in accordance with Departmental procedures, and to identify any need for process improvements as a result of common errors noted. Without formalized monitoring procedures and regular review of retained control documentation, it is difficult to control and improve the registry systems. Insufficient monitoring of registry systems could lead to undetected fraudulent activity and errors such as inaccurate land titles, invalid business registrations, or inappropriately issued permits.

Recommendation 4.1
Service Nova Scotia and Municipal Relations should formalize its management monitoring processes and include the requirement to produce and retain evidence of management review of transactions.

Recommendation 4.2
Service Nova Scotia and Municipal Relations should ensure there are procedures in place at the Land Registry to meet the monitoring requirements of the Land Registration Act Agreement with the Barristers' Society of Nova Scotia.

Privacy Policies and Procedures

Conclusions and summary of observations

Systems and processes used to protect the privacy of confidential information stored in the registries are not sufficient. There are deficiencies in communicating with staff with respect to privacy policies. Contracts, agreements and procedures relating to the Department's web-based services are not in full compliance with the Payment Card Industry Data Security Standard or the province's Personal Information International Disclosure Protection Act. Due to the sensitive nature of some of the information the registries maintain and share, communication of current policies and procedures and compliance with relevant laws and regulations is imperative to protect such information. Without these measures, exposure of confidential information related to individuals and businesses is at risk.

4.15 *Communication of policies* – There are documented policies and procedures to protect information collected and stored against unauthorized access and inappropriate disclosure. However, there are deficiencies in the communication of those policies.

4.16 There are IT policies throughout government that apply to SNSMR and they include policies to protect privacy of information. However, there is no centralized collection of IT policies at the Department. This makes it difficult for employees to be aware of, locate and follow these policies. SNSMR employees and contractors need to know what IT policies are in place to govern their use of information technology. Without knowledge of these policies, employees and contractors may misuse computer systems, intentionally or not, resulting in security vulnerabilities, and breach of privacy.

4.17 Communication of the policies that address privacy is inadequate. We found that, while there are security and privacy awareness initiatives and documents, not all staff members were aware of their existence. In addition,

staff members are informed there are policy manuals available, but privacy legislation requirements have not been added to each manual. Insufficient knowledge of the privacy requirements of current provincial legislation by staff can affect the security of private information. In addition, the Department could be found liable if there is a privacy breach and it is demonstrated that the Department did not comply with privacy laws.

Recommendation 4.3
Service Nova Scotia and Municipal Relations should ensure all of the policies and procedures necessary for the security of its information are current, communicated, and readily accessible to its staff and contractors.

4.18 *Privacy breach protocol* – The Department has a privacy breach protocol to provide direction to staff in the event of a suspected or confirmed breach of the privacy of confidential information. We found that staff members operating each of the four registries were unaware that an official protocol exists, despite it having been presented to Departmental staff members at least two months prior to our discussing this with them. Failure to ensure staff members understand the policy and its applications may result in ineffective containment of a breach of privacy, failure to notify appropriate persons of privacy incidents, no identification of issues arising from the breach, and no strategies being devised to reduce the likelihood of future breaches.

Recommendation 4.4
Service Nova Scotia and Municipal Relations should formalize its communication with and training of staff on privacy policies and the privacy breach protocol.

4.19 *Privacy impact assessments* – The Department is required to prepare a privacy impact assessment (PIA) before it makes significant changes to its information systems or implements new information technology processes. PIAs outline the likely impact of new information systems and system changes on the privacy of confidential information collected and stored by departments. Various levels of department and government management must approve PIAs. We reviewed a number of system changes at SNSMR that required a PIA and found that an approved PIA was on file for each, with no significant privacy risks identified. Discussions with staff indicated, however, that there is no formal process to ensure the implementation of recommendations for the mitigation of privacy risks identified in the approved PIA. We were informed an assurance framework that is currently under development will address this issue.

Recommendation 4.5
Service Nova Scotia and Municipal Relations should include follow-up procedures as part of its privacy impact assessment approval process to ensure any identified privacy issues are addressed before new systems or system changes are implemented.

4.20 *Credit card information processing controls* – Payment Card Industry Data Security Standard (PCI DSS) is an international information security standard defined by the Payment Card Industry Security Standards Council. The Council is a consortium of major credit card companies. The Standard identifies annual control validation requirements for any organization that processes, maintains or exchanges credit card information. The Standard also requires assessment of an organization by a third party to confirm that their information technology controls meet the Standard set by the Council. The level of testing and reporting required by each organization is dependent on the volume of credit card transactions it processes.

4.21 Based on credit card transaction volume information provided to us, the Province should be performing an annual self-assessment against the Standard, as well as obtaining a quarterly network security review from an approved vendor. Neither of these requirements has been met and therefore the Province, and all of its departments that process credit card transactions, are not PCI DSS compliant. Becoming compliant is a significant undertaking for an organization and management has told us that they have communicated with one of the major credit card companies to inform them of their plan to move toward compliance. A significant amount of the Province's credit card transactions are processed through SNSMR. Part of the Province's compliance initiative requires SNSMR to report on its state of readiness and become the baseline for all other departments that process credit cards. We were informed that this process is ongoing and all impacted departments will have tasks to complete in order for the Province to achieve compliance. This includes any infrastructure components that are the responsibility of the Chief Information Office.

4.22 *Compliance with legislation* – Government web-based services provide the public with the ability to conduct business and communicate with government through the internet. SNSMR enables businesses and the public to use the internet to see various records (e.g., public information on specific businesses), obtain specific documents (e.g., birth certificates), register interests in land, and renew business registration licenses.

4.23 SNSMR's use of web-based services results in the collection of personal information (e.g., names, addresses, credit card numbers) over the internet. Nova Scotia entities that collect such information, including all provincial departments and agencies, must adhere to the Personal Information

International Disclosure Protection Act (PIIDPA). PIIDPA is provincial legislation intended to prevent personal information from leaving Canada without the notification and consent of the person to whom the information applies. The Act also requires government departments to disclose annually to the Minister of Justice what personal information in their possession has left Canada.

4.24 SNSMR outsources the collection of credit card information for online transactions to a private-sector company. That company submits specific pieces of the information collected to companies outside of Canada for processing. Customers who submit their credit card information online are not informed that some personal information is leaving Canada and, therefore, do not have the opportunity to provide consent. In addition, for the period under audit, the Department did not inform the Minister of Justice of the transmitting of personal information outside of the country. Management informed us after the conclusion of our audit fieldwork that future annual reporting to the Minister of Justice would contain this required information.

Recommendation 4.6
Service Nova Scotia and Municipal Relations should ensure it adheres to the requirements of the Personal Information International Disclosure Protection Act and, specifically, that there is appropriate consent and reporting for all information being sent out of Canada.

Service Contracts and Information Sharing Agreements

Conclusions and summary of observations

The majority of the Department's agreements for sharing registry information with other government entities are outdated. SNSMR contracts with a private-sector company for its registry web services, but relies on the company to generate reports on their own performance. The Department does not form its own assessment of whether service providers are meeting contracted levels of performance. In addition, the Department does not obtain an independent assessment of the adequacy of its web service provider's control over the confidential information SNSMR provides.

4.25 *Inter-jurisdictional agreements to share information* – SNSMR shares information from its registries with other provincial departments and agencies, as well as other levels of government (i.e., Federal government and various municipalities). Similarly, these entities provide information to SNSMR's registries. Information shared back and forth includes items such as land transactions, information on births and deaths of Canadians while

they are outside of their home province, and business related information with various tax and workers' compensation authorities.

4.26 Our audit indicated that not all of these sharing arrangements are supported by a formal agreement as we found some for which an agreement was not finalized or signed. In addition, some of the agreements are outdated and do not reflect current standards or legislation (e.g., the Freedom of Information and Protection of Privacy Act). Without signed agreements, there is no legal requirement for either party to fulfil obligations to protect the privacy of information. This increases the risk of misuse or poor control of information shared. Updated agreements are necessary to ensure service delivery requirements are relevant and feasible. Agreements that are not current and do not reflect regulatory and privacy requirements can result in the disclosure of personal information if the level of care is not defined, and such disclosure can result in legal proceedings.

Recommendation 4.7
Service Nova Scotia and Municipal Relations should ensure no information is shared before signed agreements are in place.

Recommendation 4.8
Service Nova Scotia and Municipal Relations should monitor information sharing agreements on a regular basis to ensure they reflect all applicable standards and legislation and are relevant to current operations.

4.27 *Management and review of service contracts* – Management does not review service level agreements on a regular basis. Review generally only occurs upon recognition of a change to the services received or provided. A review of agreements on a periodic basis would help ensure they have not expired and that the terms are still valid and complied with by all entities involved.

4.28 SNSMR entered into an agreement with a company to provide e-commerce services to support SNSMR business functions. These services are very important to the core business of the registries we audited. SNSMR relies on the service provider to generate reports on the level of service provided. SNSMR cannot confirm that the reported service levels are accurate.

4.29 We also noted that SNSMR does not obtain an independent assessment of the controls that protect the financial and personal information maintained by the web service provider on SNSMR's behalf. If the Department does not receive such assessments, it cannot know whether confidential information handled on its behalf is adequately controlled.

Recommendation 4.9
Service Nova Scotia and Municipal Relations should use performance measures and other processes, including independent assurance, to determine if external service providers are meeting service level agreements and information maintained is secure.

Security Configuration Management

Conclusions and summary of observations

Security configuration settings for the IT systems that support the registries are not sufficient to prevent unauthorized access. They do not provide for logging of user actions or restrict access to various computer directories, files and programs. In addition, computer systems are at an increased risk of exploitation due to the use of programs with known security vulnerabilities. Improperly configured systems limit SNSMR's ability to ensure information it retains is secure.

4.30 *Background* – Configuration settings are the options available in computer systems that define how the computer system will function. These settings require careful management to ensure computer systems function properly. Password and user account configuration settings provide some of the key security controls of the system. These settings can include:

- whether a password is required;
- the minimum length of the password;
- the length of time the password can be used;
- whether previous passwords can be reused; and,
- the consequences of entering the wrong password too many times.

4.31 Security configuration settings also determine what information a person is able to access. This includes files, directories and even programs. If password and file settings are not appropriate, an individual could gain unauthorized access to computer systems and steal, disclose, modify or delete confidential information.

4.32 *Security application configuration* – There are two components to each registry. The application component is what users interact with for data entry, reporting and queries. The database component is where information is stored and processed. The database holding registry information is accessible independently of the application. The design of three of the four registries we examined allows an individual who has access to the

specific registry application (e.g., a registry employee) to also access the database that supports the application. Vital Statistics is the only registry that does not permit this. Only IT administrators should have access to these associated systems. There are controls within each application to restrict access to personal and confidential information. As discussed in the following paragraphs, the databases do not have the same level of control in place and as a result, data is at risk of inappropriate access.

4.33 *Security configuration standards* – The Chief Information Office is responsible for the IT networks and some of the infrastructure that host the registries (see paragraph 4.4). We assessed whether the Chief Information Office maintains configuration standards or performs reviews of existing computer settings to ensure the security of the systems hosting the registries. We found there are no documented security configuration standards, and that settings for systems supporting the registries are inconsistent.

4.34 *Security configuration settings* – Both the Chief Information Office and the Department have configuration responsibilities for specific components of the registries' computer systems. We examined security configuration settings of the network, registry applications, operating systems and databases to determine if the settings appropriately prevent or detect unauthorized access to the systems. Some of the systems do not sufficiently log use of the computer systems. Therefore, detection of unauthorized access is not possible. We also noted that operating systems used on computers supporting registry systems contain security vulnerabilities that could allow them to be hacked. These include the use of vulnerable programs, weak password and account settings, as well as inappropriate file and directory access permissions. Based on the findings described in the following paragraphs, we concluded that control over the prevention of unauthorized access is weak.

4.35 *Logging* – Maintaining a record of computer system use provides management with information to investigate fraud or unauthorized actions by employees. It also provides them with the ability to determine if registered system users still require their computer accounts. We found that 17 of the 19 systems supporting SNSMR registries do not record sufficient information on system user activity.

4.36 *Clear text services* – Some programs send confidential information such as user names and passwords, computer commands and data files over the network without first encrypting the information. Interception of such information could provide a person with inappropriate access to a system or the ability to read personal and confidential information. The service can also be utilized by hackers to transfer files to and from the server once the server has been compromised. We identified six registry-hosting servers with these programs enabled through configuration settings.

4.37 *Password settings* – Access to a computer system requires a user name and a password. The password prevents unauthorized use of an account by others. However, individuals could attempt to crack a password by employing software that tries all possible character (e.g., upper and lower case letters, numbers) combinations. Longer passwords, and more types of characters used, increases the number of combinations and time required to crack the password. This increases the level of security associated with the password.

4.38 We assessed the password and user account settings for the registry applications, the operating systems running the applications, and the databases that store registry information. We noted that the registry applications do require the use of passwords and user accounts to restrict access to only authorized users. However, the password settings for the operating systems and databases managed by SNSMR do not prevent users from using weak passwords.

4.39 We obtained a copy of the system password file and used a password-cracking tool to determine if the accounts on the operating systems contained weak passwords. The tool was able to crack the password of four user accounts within a 20-hour period. Being able to crack even one password poses a risk to system security.

4.40 SNSMR's password configuration settings generally follow the government's wide-area network password policy. However, we identified some network user accounts that do not comply with this policy. We examined 1,472 accounts and found 12 that do not meet the minimum password length policy and six that do not force the account to require a password. These accounts could potentially have very weak or no passwords, providing easy access to computer systems by individuals operating within the government network.

4.41 *Password expiration* – Password expiration settings define how long users can use their passwords before they are required to change them. Changing passwords on a periodic basis helps reduce the risk of the inappropriate use of a compromised password for extended periods. We reviewed the administrator accounts for the systems supporting the registries to identify the most recent password changes. Our analysis found administrator accounts with passwords unchanged over a time span between seven months and four years. In addition, we found one administrator password unchanged since activation.

4.42 *Password history* – Password history settings can define how many different passwords a user must use before allowing them to reuse a previously expired password. If users can frequently reuse old passwords, previously stolen passwords are at risk of reactivation, providing unauthorized access

to the systems. We noted that systems hosting the registries do not prevent users from reusing recently used passwords.

4.43 *Simultaneous login* – The simultaneous login settings define how many times a person can use their user name and password on multiple computer systems at the same time. If a person can sign into different computer systems at the same time, there is a greater risk they may share their user name and password with another individual. Employees may decide to provide access to others who are assisting them or to those who can no longer use their own account. This could provide that individual with the ability to obtain unauthorized access to information. We reviewed the network setting that allows simultaneous logins and noted settings ranged from one to 34 times.

4.44 *File and directory permissions* – File and directory permissions are the settings that define what information or computer programs a user or groups of users can access on a computer system. If these settings are not appropriate, a user could gain access to information not needed to fulfil their day-to-day responsibilities. Our analysis of file and directory permissions identified that system users could gain access to specific system programs, database configuration files, process schedulers and encryption keys that they do not require.

4.45 Management informed us that the current wide-area network standards address some, but not all, of these issues. However, some of the registry systems were implemented before these standards came into effect. As these systems undergo periodic maintenance, their security configuration settings should be updated.

Recommendation 4.10
The Chief Information Office should update security configuration standards based upon industry best practices and require that all government system security configurations be realigned with these standards during the system maintenance life cycles.

Identity and Access Management

Conclusions and summary of observations

There are deficiencies in the management of user access to the registries. No process is in place to identify and remove dormant user accounts. The process to manage access is inconsistent across all registries. Processes relating to the termination and expiration of user accounts are inadequate, and procedures for issuing and changing temporary passwords are poor. The configuration of network accounts belonging to external contractors and consultants needs improvement.

4.46 *Background* – Access management is the process of providing employees with computer accounts, setting and changing their ability to access different types of information, and removing computer accounts when employees are no longer with the organization. Employees only need the level of access that allows them to perform their job. Those with more access than necessary have an increased ability to see confidential information or commit fraud. Employees terminated by an organization could retaliate by disclosing, modifying or deleting sensitive information if deactivation of their user accounts does not occur at the time of their termination.

4.47 *Access management process* – There are currently, at minimum, three different processes within SNSMR to manage access to the network and the registries. Two of the four registry business units handle their own access requests, while the network and the other two registries use external service desks to facilitate the management of access. During our audit, service desk responsibility transferred from the Department of Community Services to the Chief Information Office. Multiple processes to manage access requests decrease the ability of management to grant and terminate access appropriately.

4.48 *Vital statistics* – Managing access to the Vital Statistics registry occurs at the division level within SNSMR. Access levels and roles are defined and approved by authorized division staff. After a new user has been created through the service desk and a network identity has been assigned, department staff members enter the required information and assigned network identity into the provincial identity management system. This provides the user with the approved level of access to the Vital Statistics registry. Division management regularly confirm all users are current and that assigned access privileges are appropriate for their job responsibilities. We reviewed user access to the system and found that all users were active employees and their assigned access privileges were appropriate.

4.49 *Land Registry* – The Land Registry can provide two levels of access: query access and submission access. Query access allows a user to view information, but not change it. Submission access allows a user to submit information for recording in the database. Users who are lawyers and require submission access must have specific prerequisites (e.g., member of the Nova Scotia Barristers' Society) documented before SNSMR provides access. We reviewed files for 15 lawyers with submission access and found that there was documented evidence of the required prerequisites for each of them.

4.50 We noted that Land Registry staff generate user names and passwords, and store them centrally in an electronic document. The document is not password protected and is available to four Land Registry staff members and network administrators. In the event that unauthorized individuals

access the password document, they would have access to all user accounts and have the ability to submit electronic documents online without proper authorization. Further, when new users log in, the system does not force them to change their initial, temporary password.

4.51 Users with multiple accounts increase the difficulty for administrators to manage access and could result in active accounts being accessible to unauthorized users. We noted 146 individuals who had multiple user accounts to access the registry. This also increases the pervasiveness of dormant accounts as discussed in paragraph 4.53.

Recommendation 4.11
Service Nova Scotia and Municipal Relations should regularly review all of its Land Registry accounts to ensure deletion of unnecessary duplicate accounts, deactivation of dormant accounts, and changing of the initial, temporary password.

4.52 *Access management* – An external service desk (see paragraph 4.4) provides help desk services to SNSMR to facilitate access to the wide-area network, the Nova Scotia Business Registry, and the Registry of Joint Stock Companies. However, for registry access, they forward the request to the SNSMR registry business unit to approve and administer. We selected a sample of 44 employees who had either joined, transferred to another department, or were terminated from SNSMR, and reviewed their system access request and termination forms. We found the following areas of concern.

- Issuance of the same temporary password for network access to new employees occurs frequently. Individuals with knowledge of this practice could inappropriately access a new employee's account before the temporary password is changed and review, copy or change information anonymously.
- Access was granted to two registries for one employee but there was no application request form on file.
- Network access privileges set up for new users are often copies of privileges granted to similar employees. This speeds up the process. We saw no evidence of a review of such access privileges prior to copying to ensure they were appropriate for the new user. By copying an existing employee's permissions in this manner, there is a risk that new employees may obtain more system access than is required to perform their job.
- There was no termination request form on file for five of twenty employees terminated. The removal of access privileges may not

happen if the service desk does not receive formal termination request forms.

- The removal of access for fifteen of the twenty former employees with termination request forms on file was, on average, five days after the termination date stated on the form. Employees leaving the Department could use their access during this period to copy, modify or delete important registry information.

- Seventy of seventy-two external contractors and consultants identified in our examination did not have their network passwords set to expire after a set length of time. The use of a contractor is typically a defined-term arrangement. Setting contractor user accounts to expire after a specified period ensures contractors no longer have access when they are not providing services to the Department.

Recommendation 4.12
The Chief Information Office should generate unique temporary passwords for all new system accounts to prevent inappropriate access to new accounts before the passwords are changed.

Recommendation 4.13
Service Nova Scotia and Municipal Relations should review termination listings from its human resources division on a regular basis to verify the removal of network and registry user accounts belonging to terminated employees.

Recommendation 4.14
Service Nova Scotia and Municipal Relations should establish a process to ensure user accounts for external contractors are set to expire after a specified period to ensure contractors no longer have access when they are no longer providing services to the Department.

4.53 *Dormant accounts* – Dormant accounts are computer accounts that belong to employees who have not used their accounts for a significant period or accounts which have not been disabled or deleted and are associated with individuals who are no longer with the organization. These user accounts remain functional and available for use. An individual with knowledge of the user name and password of a dormant account could use that account to gain unauthorized access to information (see the Security Configuration Management section starting on page 65 for findings regarding passwords). We analyzed user accounts for the network, the various registries, the supporting operating systems, and the databases. Our analysis identified a significant number of dormant accounts on these systems.

- 9.8% of all SNSMR network accounts had never been logged into.
- 17.1% of all SNSMR network user passwords had expired.
- 12.6% of all Registry of Joint Stock Companies accounts were dormant.
- 11.6% of all Business Registry accounts were dormant.
- 8.25% of the accounts for the computer servers supporting the registries were dormant.
- There were no dormant accounts for the Registry of Vital Statistics.

4.54 Administrators should routinely identify and eliminate such accounts, ensuring few or no dormant accounts exist.

4.55 The Land Registry does not maintain a record of when users last accessed the registry. As a result, management cannot review system-generated reports to identify dormant accounts. We selected a sample of accounts and reviewed them with management to determine the employment status of the account owner. Through this testing, we identified 28 functional accounts for individuals no longer working for the registry. Three of these are of higher risk to system security because they are administrator accounts, which come with more authority for making system changes and accessing confidential system information.

4.56 The following are best practices that could mitigate the weaknesses identified above.

- On a quarterly basis, identify all accounts that have not accessed the system for a predetermined period.
- On a quarterly basis, obtain a formal listing from Human Resources of all terminated employees since the last user account review to ensure there are no active accounts belonging to terminated employees.
- Annually validate that all existing employee user accounts provide only the access employees require to fulfil their job responsibilities. This will usually require communication with the managers or supervisors of system users to have them review for changes in job responsibilities during the year.

Recommendation 4.15
Service Nova Scotia and Municipal Relations should ensure there is a process in place that requires the following:

- configuration of its systems to include logs and reports of when user accounts were last accessed;
- regular reviews of reports and logs;
- regular reviews of user accounts and associated access privileges for all existing networks, applications, operating systems and databases; and
- procedures to determine if the owner of an account still requires access, or if certain access privileges need modification or termination.

Patch Management

Conclusions and summary of observations

There is inadequate patching of the registries' computer systems. We assessed whether SNSMR and the Chief Information Office have a process to identify and apply patches provided by software vendors for the systems that support the registries. We concluded that there are limited documented procedures to review and implement vendor patches in a timely manner.

4.57 *Background* – Software sold or freely provided by vendors can have flaws that require correction. These flaws can negatively affect computer system performance and can create security vulnerabilities. Individuals with malicious intent research these flaws and attempt to use them to hack computers. To help prevent this from occurring, vendors routinely provide fixes (patches), or groups of fixes (service packs). These fixes should be applied shortly after a vendor provides them in order to reduce the opportunity for someone to use the flaw to hack a computer system. A hacker could affect the availability, confidentiality and integrity of information contained within systems.

4.58 *Patches* – We found that only nine of 36 operating systems supporting SNSMR registries and the government's network had all current patches or service packs implemented. Patching of the remainder of the systems is behind by up to three years.

4.59 One system's vendor releases patches for its database software every three months. There was no evidence these updates were applied to SNSMR's databases during our audit testing period from September 1, 2008 to September 30, 2009.

Recommendation 4.16
Service Nova Scotia and Municipal Relations and the Chief Information Office should develop a process for identifying, reviewing and implementing patches to their software in a timely manner utilizing Information Technology Infrastructure Library best practices.

Change Management

Conclusions and summary of observations

We assessed SNSMR's process for making changes to its computer systems and concluded there is a well-designed process in place. However, some enhancements are required to ensure the retention of documentation for all changes made and approvals granted. We also noted that the development of some web applications does not always follow secure programming practices that ensure the applications do not contain exploitable vulnerabilities to hack SNSMR websites or other computer systems.

4.60 *Background* – Change management is the formal process to add, modify or remove information technology from an organization. This process requires testing and approval of changes prior to implementing them on the computer systems used by employees or customers. Such processes reduce the risk of changes negatively affecting the performance of a system, and prevent employees from making changes to computer programs to commit fraud or access confidential information without proper authorization.

4.61 *Change management process* – On March 1, 2009, SNSMR implemented a new process for making changes to computer systems. We found the new process to be well designed. However, we also found that parts of the new process are not being followed. We reviewed a sample of 40 system changes to determine if they were tested, approved and sufficiently documented to support the change. We identified the following issues.

- Management did not provide approval to move system changes from a test environment into the production (live) environment for three of the 40 changes tested. Emergency changes accounted for two of the three exceptions and management indicated that approvals were verbal. The other change occurred during the initial stages of implementing the new change management process.
- SNSMR requires approval of emergency system changes by a group of advisors known as the Emergency Change Advisory Board. We saw no evidence that this group reviewed the emergency changes in our sample.

- There is no review by management to ensure retention of all significant documentation, including all approvals, to support system change.
- Two application programmers have access to operating systems supporting the registries. Programmers with access to these systems could create and implement changes without obtaining proper authority.

Recommendation 4.17
Service Nova Scotia and Municipal Relations should perform a periodic review of system changes to ensure the retention of all required approvals, testing results and other key documentation.

Recommendation 4.18
Service Nova Scotia and Municipal Relations should review all access provided to programmers to ensure there is not a segregation of duties risk that could allow the programmer to develop and implement code without authorization.

4.62 *Secure development* – We identified that web application programming does not comply with industry-standard secure coding techniques such as the Open Web Application Security Project (OWASP). Such techniques help prevent security vulnerabilities that could be attacked over the internet to illegally gain access to Department systems. We found that security vulnerabilities exist in the web applications for one of the registries. An external service provider hosts websites for the other three registries and our assessment did not extend to the practices of this private-sector company.

Recommendation 4.19
Service Nova Scotia and Municipal Relations should use industry-standard secure coding techniques and perform security assessments to prevent security risks in its web applications.

Project Management

Conclusions and summary of observations

SNSMR has a well-designed, documented process for managing projects. We found that more management oversight is required to ensure all documentation required by the process is prepared and retained.

4.63 *Background* – Projects are changes in an organization that require a significant amount of time or money to complete. In order for implementation of these changes to be as planned, timely and on budget, a formal process is required to track and manage the project from planning to completion. Improperly managed IT projects can result in cost overruns, missed deadlines, service interruptions, increased security risks, or implementation of information technology that does not meet the needs of its users.

4.64 *Project management framework* – SNSMR has developed a framework to guide projects from initiation to completion. This framework includes steps to ensure the approval, planning, documentation, testing and implementation of projects. We concluded that the framework is well designed and appropriately documented.

4.65 *Active projects* – SNSMR had 48 active projects during the period of our audit. These resulted from information technology upgrades, new legislative requirements, business process re-engineering, and the automating of business processes. We examined two projects from the seven completed during the period of our audit and noted the following.

- There was no evidence of a formal documented risk assessment for one of the projects. However, various documents outlined potential risks associated with the project. Failure to perform a formal risk assessment prior to implementing new technology could introduce vulnerabilities that may be exploited and affect the overall security of Department systems.

- There was no lessons learned document available for one of the projects. SNSMR's project management framework requires preparation of such a document upon the completion of a project. Documenting successes and shortcomings within a project enables managers to learn from previous mistakes and to employ new best practices that increase the success of projects.

Recommendation 4.20
Service Nova Scotia and Municipal Relations should develop processes which ensure all required documentation, as outlined in the Department's project management framework, has been produced or obtained for system development projects.

Incident and Problem Management

Conclusions and summary of observations

We concluded that SNSMR has a process to address computer problems. However, this process does not include the identification and long-term resolution of the root cause of recurring computer problems to prevent future occurrences.

4.66 *Background* – Incident management is the process of identifying and resolving any IT-related event that has a negative impact on an organization's operations. This process focuses primarily on fixing the issue and not attempting to determine why it occurred. Problem management is the process to investigate why the incident occurred in the first place and to attempt to fix the issue that caused the incident. If these processes are not in place, extended interruption of the information services could result.

4.67 *Incident management* – At the time of our fieldwork the Department of Community Service's Help Desk received calls from SNSMR system users to report computer incidents. The Help Desk recorded all relevant information in their ticket (service request) tracking software. For issues that related to SNSMR computer systems, the Help Desk forwarded the ticket to a SNSMR IT specialist to be resolved. However, the process to document and respond to these events did not require classification of security incidents according to level of impact or provide response plans according to the severity of the incident. This can reduce the ability of staff to respond appropriately to incidents.

4.68 *Problem management* – We found that SNSMR does not have a problem management process to identify and address the root causes of incidents.

4.69 *Help desk software* – The ticket tracking application used by the Help Desk did not have the ability to identify and report SNSMR-specific issues. Without this ability, it is difficult to look for potential larger issues that could indicate there is a system weakness that is causing multiple computer incidents to occur.

Recommendation 4.21
Service Nova Scotia and Municipal Relations should have formal, documented problem and incident management processes. This should include using help desk software that can identify recorded incidents specific to the Department and provide sufficient reporting to allow for the analysis of such incidents.

Business Continuity and Disaster Recovery Planning

Conclusions and summary of observations

There are deficiencies in the Department's planning for the maintenance of business services and restoration of computer systems in the event of a prolonged interruption in the availability of important computer systems. SNSMR has a formal business continuity plan, but it is not complete. The Department also has a disaster recovery plan, but it is still in a draft state. The Chief Information Office does not have a formal disaster recovery plan for its datacentre, which hosts the registries of SNSMR.

4.70 *Background* – Organizations require formal plans for the maintenance and restoration of business functions and the information technology that supports them in the event of a disaster. If such plans are not in place, there is a risk that services provided by the organization will be unavailable for an excessive length of time.

4.71 *Business continuity plan* – A business continuity plan assigns a priority to services provided by an organization and outlines a plan to restore those services from the highest to lowest priority in the event of a disaster. This could include moving to a new location, outsourcing services to another organization, or using paper-based processes in place of computer systems. SNSMR has a documented business continuity plan, but the action plans specific to the various business units to restore business services are incomplete.

4.72 *Disaster recovery plan* – We noted that SNSMR has a draft version of a disaster recovery plan and cannot finalize the plan without a service-level agreement with the provincial datacentre, which is managed by the Chief Information Office. SNSMR relies on the datacentre to operate the computers that support its registries and, without a service-level agreement, the Department does not have the documentation that describes the responsibility of each party to resume registry operations in the event of a disaster.

4.73 We also noted that the Chief Information Office does not have a formal, documented disaster recovery plan. Datacentre management indicated that there are informal plans and processes to restore computer systems.

Recommendation 4.22
Service Nova Scotia and Municipal Relations should complete the outstanding items in its business continuity plan, provide training to all relevant employees, and test the plan.

Recommendation 4.23
Service Nova Scotia and Municipal Relations should negotiate system restoration times and services with the Chief Information Office to allow for the completion of its disaster recovery plans.

Recommendation 4.24
The provincial datacentre, which is managed by the Chief Information Office, should document a formal disaster recovery plan for the restoration of its systems in the event of a disaster.

Response: Service Nova Scotia and Municipal Relations

Service Nova Scotia and Municipal Relations (SNSMR) is pleased to provide a response to the Auditor General's review of Registry Systems. We appreciate the extensive work done by the Auditor General's staff to identify areas that can be improved in the management of these registries. This review has provided SNSMR with a number of recommendations that when implemented, will improve registry operations and reduce the risk of unauthorized access to registry information.

SNSMR recognizes the importance of minimizing the risk of unauthorized access to its electronic registries and has put in place extensive measures to protect access to its registries. There is no indiction from either the audit or from the department's experience that any of the deficiencies identified in the review have resulted in any unauthorized access to registries. We generally agree with the report's conclusion that the recommendations for improving information technology controls will require relatively minimal resources to implement. The recommendations are focused on configuration changes to existing systems and additional policies and procedures. SNSMR will be working closely with the CIO to ensure that these recommendations are implemented in a timely manner.

The Auditor General's recommendations for SNSMR are accepted in principle and work has begun to put these in place. We are confident that the implementation of these recommendations will strengthen both the business process and information technology controls for the registries.

Recommendation 4.1
Service Nova Scotia and Municipal Relations should formalize its management monitoring processes and include the requirement to produce and retain evidence of management review of transactions.

SNSMR accepts this recommendation. A formal management review process will be developed and implemented to assess transaction quality. The results of these reviews will be documented and retained according to departmental records management practices.

Recommendation 4.2
Service Nova Scotia and Municipal Relations should ensure there are procedures in place at the Land Registry to meet the monitoring requirements of the Land Registration Act Agreement with the Barristers' Society of Nova Scotia.

SNSMR accepts this recommendation.

Recommendation 4.3
Service Nova Scotia and Municipal Relations should ensure all of the policies

and procedures necessary for the security of its information are current, communicated, and readily accessible to its staff and contractors.

SNSMR accepts this recommendation. All corporate and departmental policies and procedures related to information security and privacy will be made available electronically at a single centralized location.

A communications strategy will also be developed to make staff aware of these policies and procedures.

Recommendation 4.4
Service Nova Scotia and Municipal Relations should formalize its communication with and training of staff on privacy policies and the privacy breach protocol.

SNSMR accepts this recommendation.

Recommendation 4.5
Service Nova Scotia and Municipal Relations should include follow-up procedures as part of its privacy impact assessment approval process to ensure any identified privacy issues are addressed before new systems or system changes are implemented.

SNSMR accepts this recommendation.

Recommendation 4.6
Service Nova Scotia and Municipal Relations should ensure it adheres to the requirements of the Personal Information International Disclosure Protection Act and, specifically, that there is appropriate consent and reporting for all information being sent out of Canada.

SNSMR accepts this recommendation with the following clarification.

With respect to credit card information being sent outside Canada, it has been SNSMR's position that appropriate consent occurs in the agreement between the customer and the credit card issuer. Therefore SNSMR has been in adherence to the requirements of the Personal Information International Disclosure Protection Act. The Canadian Privacy Commissioner's findings for PIIDPA Case #2005-313 for CIBC Visa is seen to support this position.

SNSMR's future PIIDPA reports to the Minister of Justice will now identify credit card transaction information being sent outside Canada.

SNSMR will also publish a notice in its online services informing customers of the possibility that their credit card information may be sent outside of Canada for processing.

RESPONSE: SERVICE NOVA SCOTIA AND MUNICIPAL RELATIONS

Recommendation 4.7
Service Nova Scotia and Municipal Relations should ensure no information is shared before signed agreements are in place.

SNSMR supports this recommendation and will develop a process to ensure that all agreements contain the necessary signatures.

Recommendation 4.8
Service Nova Scotia and Municipal Relations should monitor information sharing agreements on a regular basis to ensure they reflect all applicable standards and legislation and are relevant to current operations.

SNSMR supports this recommendation and will review information sharing agreements on a regular basis, with input from legal counsel, to ensure they reflect all applicable standards and legislation.

Recommendation 4.9
Service Nova Scotia and Municipal Relations should use performance measures and other processes, including independent assurance, to determine if external service providers are meeting service level agreements and information maintained is secure.

The company with which SNSMR has contracted e-commerce services meets on a monthly basis with departmental staff to review performance measures. In addition, a quarterly independent vulnerability assessment is completed as part of their requirement to provide PCI-DSS compliance. SNSMR will request that the company provide a summary of the vulnerability assessment be made available to the department for review.

Recommendation 4.11
Service Nova Scotia and Municipal Relations should regularly review all of its Land Registry accounts to ensure deletion of unnecessary duplicate accounts, deactivation of dormant accounts, and changing of the initial, temporary password.

SNSMR accepts this recommendation and will develop a procedure to regularly review Land Registry accounts.

Recommendation 4.13
Service Nova Scotia and Municipal Relations should review termination listings from its human resources division on a regular basis to verify the removal of network and registry user accounts belonging to terminated employees.

SNSMR accepts this recommendation.

Recommendation 4.14
Service Nova Scotia and Municipal Relations should establish a process to ensure user accounts for external contractors are set to expire after a specified period to ensure contractors no longer have access when they are no longer providing services to the Department.

SNSMR accepts this recommendation.

Recommendation 4.15
Service Nova Scotia and Municipal Relations should ensure there is a process in place that requires the following:

- ***configuration of its systems to include logs and reports of when user accounts were last accessed;***
- ***regular reviews of reports and logs;***
- ***regular reviews of user accounts and associated access privileges for all existing networks, applications, operating systems and databases; and***
- ***procedures to determine if the owner of an account still requires access, or if certain access privileges need modification or termination.***

SNSMR agrees with this recommendation and will work with the CIO to ensure that this process is in place.

SNSMR will also continue to improve its current user account lifecycle management processes to ensure that all network, applications, operating system and database accounts are current and assigned the appropriate privileges.

Recommendation 4.16
Service Nova Scotia and Municipal Relations and the Chief Information Office should develop a process for identifying, reviewing and implementing patches to their software in a timely manner utilizing Information Technology Infrastructure Library best practices.

SNSMR accepts this recommendation. SNSMR has developed an application patch management process and will work closely with the CIO to ensure this process is integrated into their infrastructure patch management process.

Recommendation 4.17
Service Nova Scotia and Municipal Relations should perform a periodic review of system changes to ensure the retention of all required approvals, testing results and other key documentation.

SNSMR accepts this recommendation.

Recommendation 4.18
Service Nova Scotia and Municipal Relations should review all access provided

to programmers to ensure there is not a segregation of duties risk that could allow the programmer to develop and implement code without authorization.

SNSMR accepts this recommendation in principle. SNSMR has implemented a full change management process based on the ITIL framework. The ability to fully implement this recommendation will be dependent on staff levels.

RESPONSE: SERVICE NOVA SCOTIA AND MUNICIPAL RELATIONS

Recommendation 4.19
Service Nova Scotia and Municipal Relations should use industry-standard secure coding techniques and perform security assessments to prevent security risks in its web applications.

SNSMR accepts this recommendation.

SNSMR has conducted security vulnerability assessments on its recent web application implementations, and will develop a process to continue such assessments for new or changed applications in the future. This will be accomplished either through the acquisition of an appropriate suite of assessment tools or through contracting an external service provider to perform the assessments on our behalf.

Recommendation 4.20
Service Nova Scotia and Municipal Relations should develop processes which ensure all required documentation, as outlined in the Department's project management framework, has been produced or obtained for system development projects.

SNSMR accepts this recommendation.

Recommendation 4.21
Service Nova Scotia and Municipal Relations should have formal, documented problem and incident management processes. This should include using help desk software that can identify recorded incidents specific to the Department and provide sufficient reporting to allow for the analysis of such incidents.

SNSMR accepts this recommendation in principle.

SNSMR has had incident management processes in place since 2007.

The ability to fully implement problem management processes may be limited due to the requirement for additional staff resources and/or investments.

Recommendation 4.22
Service Nova Scotia and Municipal Relations should complete the outstanding

items in its business continuity plan, provide training to all relevant employees, and test the plan.

SNSMR accepts this recommendation. SNSMR has a very robust business continuity plan that has been rolled out to management and the remaining staff will receive training and information before December 2010. Part of the ongoing maintenance of the plan will include testing, updating, and continuous improvements.

Recommendation 4.23
Service Nova Scotia and Municipal Relations should negotiate system restoration times and services with the Chief Information Office to allow for the completion of its disaster recovery plans.

SNSMR accepts this recommendation.

Response: Chief Information Office

The Chief Information Office would like to thank the staff of the Auditor General for their courtesy and professionalism while conducting this audit. One of the responsibilities of the Office is to supply infrastructure support services to departments including Service Nova Scotia and Municipal Relations. We are committed to providing quality secure services to our client departments.

RESPONSE: CHIEF INFORMATION OFFICE

The Chief Information Office has recently taken on the support responsibilities from the Corporate Service Units and from Corporate IT Operations for a good deal of government's infrastructure. Much of the efforts to date have been in rationalizing infrastructure and services, simplifying our technical environment and continuously working to evolve and advance our security measures as technology changes.

Currently we are focused on adopting industry recognized ITIL best practices for the processes that support the infrastructure environment as well as working to define standards for technology solutions and applications.

The Auditor General's four recommendations related to the Chief Information Office are accepted in principle. The results of the audit will be forwarded to the appropriate Technology and Information governance committees. The Office, as secretariat support to governance, and as corporate service providers will investigate COBIT and ITIL in order to provide advice in determining next steps.