3 Government-wide: Information Technology Security

Summary

Our government-wide audit of aspects of IT security identified significant deficiencies in IT security planning, monitoring and policy enforcement, as well as a need for improved policies and standards. If government systems are not adequately protected they may be compromised from within government or from anywhere in the world by those skilled at infiltrating and attacking IT systems.

During our audit of IT Security, we noted government had made a significant and positive move in creating the position of Chief Information Officer. However, the role of this position has not yet been fully defined. The organizational structure for government's IT operations remains confusing and onerous. We also observed the need for a decision on a centralization project that has been in progress for several years, the strengthening of authority for ensuring government-wide IT policies and projects are acted upon, and changes to where the function which oversees government's IT security is to report.

Planning for IT security is not adequate. We identified the need for an IT security oversight committee, corporate IT security charter and corporate IT security plan. Government-wide data classification standards are also needed.

Security policies and standards require strengthening. There is no government-wide acceptable use policy, the threat risk assessment process guide is out of date, and laptop security guidelines lack the authority of policy and do not address the securing of all mobile computing devices.

We observed instances in which government IT security policies are not being complied with. There have been insufficient numbers of threat risk assessments performed and inadequate security training for computer users.

Practices for monitoring and enforcing compliance with corporate IT policies and standards are not adequate. We identified areas for improvement, including more attention to the cost and benefits of network monitoring devices, the formalization of the government's computer emergency response team, and better security over the use of wireless internet access.

3 Government-wide: Information Technology Security

Background

GOVERNMENT-WIDE: INFORMATION TECHNOLOGY SECURITY

3.1 Information technology (IT) has evolved rapidly since the 1960's when its capabilities began gaining wide recognition as a means of producing significant efficiencies by automating manual business processes. We have come a long way since those early days; IT has now gained significant prominence as a strategic and critical business enabler. There are now virtually no significant business processes in any large organization that are not dependant on IT. Today it is nearly impossible for an organization to function efficiently and effectively in a globally-connected economy without extensive reliance on IT. However, this level of influence of IT on business brings with it several risks; many of which evolve as rapidly as IT does.

3.2 Before IT gained prominence in the business world, security over sensitive information was primarily a physical endeavour. Important documents were simply kept under lock and key, and those needing access either had possession of the keys or had to ask permission to access the documents. Either way, the documents rarely left the physical location where they were maintained, and care and custody of the information was relatively easy to maintain.

3.3 Today, information collected, processed and managed by IT systems is far more challenging to protect since it is now at risk as a result of global electronic connectivity. If it is not properly protected, information can be accessed from anywhere in the world by those skilled in infiltrating and compromising IT systems. In many cases, information is no longer gathered for a single purpose. Information is commonly used by multiple business applications and shared across geographic boundaries. This adds significantly to the risks to which it is exposed.

3.4 The IT Governance Institute, in its publication *COBIT Security Baseline, 2nd Edition*, defines information security as:

> *"Security relates to the protection of valuable assets against unavailability, loss, misuse, disclosure or damage…The information must be protected against harm from threats leading to different types of impacts, such as loss, inaccessibility, alteration or wrongful disclosure. Threats include errors and omissions, fraud, accidents, and intentional damage…"*

GOVERNMENT-WIDE: INFORMATION TECHNOLOGY SECURITY

3.5 The government of Nova Scotia relies extensively on information technology. Approximately 10,000 employees operate computers. In 2007-08, government budgeted approximately $100 million for its computer operations and infrastructure purchases. Virtually every government department, agency and program would be adversely and significantly affected by a loss of its computer processing ability due to an IT security incident.

3.6 In addition, government is entrusted with information relating to thousands of businesses and hundreds of thousands of citizens. Citizen-related information includes vital statistics; driver's licenses and records; criminal records; grant and income assistance records; and health records, just to name a few. Business-related information includes ownership records; permits and licenses; financial information; as well as various planning and marketing information. Much of this information is highly sensitive and requires a great deal of care and diligence in maintaining its confidentiality.

3.7 The February 2008 Report of the Auditor General described the results of an audit of information technology governance and concluded that the government's IT governance structures were not adequate. IT security is a subset of IT governance. It is crucial that security be high on the agenda of senior officials and Executive Council, with full recognition of the importance of promoting and providing a security-conscious organization. The IT Governance Institute, in its publication *Information Security Governance – Guidance for Boards of Directors and Executive Management*, states: *"To achieve effectiveness and sustainability in today's complex, interconnected world, information security must be addressed at the highest levels of the organization, not regarded as a technical specialty relegated to the IT Department."*

Audit Objectives and Scope

3.8 In February 2009 we completed a government-wide audit of aspects of IT security. The audit was conducted in accordance with Section 8 of the Auditor General Act and auditing standards established by the Canadian Institute of Chartered Accountants.

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

- information technology security planning at the corporate and departmental levels of government;
- information technology security policies and standards at the corporate and departmental levels of government; and

- management practices for monitoring and enforcing compliance with information technology security policies and standards.

3.10 We used the IT Governance Institute's framework COBIT 4.1 to formulate the objectives and evaluation criteria for the audit. COBIT 4.1 is a widely accepted international source of best practices for the governance, control, management and audit of information technology. These objectives and criteria were discussed with, and accepted as appropriate by, key members of government's corporate IT functions.

3.11 Our audit focused on the Nova Scotia government's framework and practices for providing and maintaining a secure technology infrastructure. Detailed testing of government-wide compliance with specific security policies and standards, and evaluation of network security measures implemented were not included in this audit. These areas will be considered in our planning for future audits.

Significant Audit Observations

Framework for IT Security

Conclusions and Summary of Observations

Government made a significant and positive move in creating the position of Chief Information Officer, which will hopefully result in stronger leadership and clearer lines of authority for the governance and management of information technology. The organization, responsibilities and authorities of this new position have not yet been finalized. In the meantime, the organizational structure for government's IT operations is still confusing and onerous. We also observed the need for a decision on a centralization project that has been in progress for several years, the strengthening of authority for ensuring government-wide IT policies and projects are acted upon, and improvements to the reporting and resourcing of the function which oversees IT security for the government's wide area network. We believe the new Chief Information Officer position is well situated to address these and all of the other findings and recommendations of this audit, other than the one directed towards Executive Council.

3.12 *Organizational framework* – We identified a need to examine the organizational framework for government's IT operations as part of this audit because it has a significant impact on the ability of government to adequately plan for IT security, as well as create and enforce government-wide policies and standards. Poor organization can result in a lack of clarity regarding where the responsibility for security planning, monitoring and enforcement lies, and the availability of resources to carry out these activities.

3.13 The February 2008 Report of the Auditor General included the results of an audit of IT governance where we concluded that government's IT governance framework was inadequate. We provided several recommendations focused on establishing a framework. A specific area of concern was the confusing corporate organizational structure for its various information technology functions.

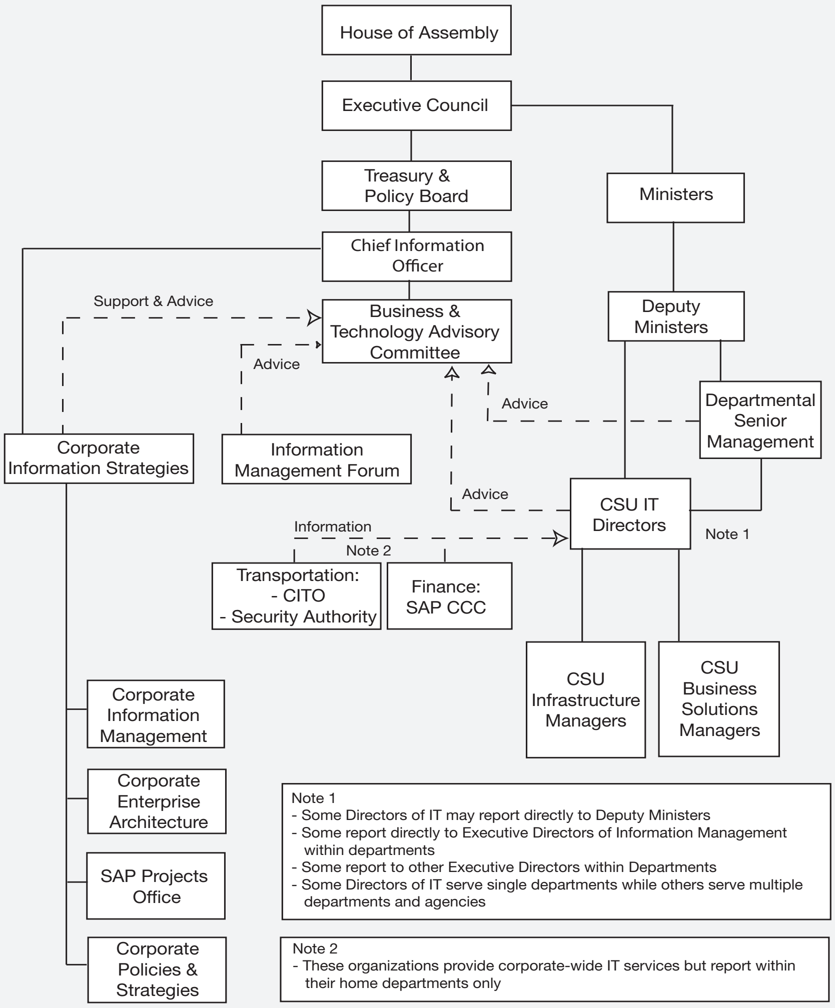
3.14 On November 27, 2008 a government news release announced the appointment of a person to the dual role of Deputy Minister of Treasury and Policy Board, and Chief Information Officer (CIO) for government, which both became effective on December 8, 2008. The appointment of a CIO has the potential to have great significance because it represents a new source of leadership and authority for government's IT operations. Although the role of CIO in the Nova Scotia government had not been fully defined at the time of our audit, it has potential to have a significant impact on the corporate IT environment of the government.

3.15 At the time of our audit, the following positions and groups were assigned a role in information technology and its security.

- Business Technology Advisory Committee
- Chief Information Officer
- Corporate Information Strategies
- Corporate Information Technology Operations
- Corporate Service Units – IT Divisions (8)
- Information Management Forum
- IT Directors Forum
- IT Infrastructure Managers Forum
- SAP Competency Centre
- Wide Area Network Security Authority

3.16 These groups operate in an environment exhibiting features of both a centralized and decentralized corporate IT framework. The following chart provides an overview of the corporate IT organization, including the role of the new CIO as it was positioned at the time of our audit.

Information Technology Organization Overview – March 2009


House of Assembly
Executive Council
Treasury & Policy Board
Ministers
Chief Information Officer
Support & Advice
Business & Technology Advisory Committee
Deputy Ministers
Advice
Advice
Departmental Senior Management
Corporate Information Strategies
Information Management Forum
Advice
CSU IT Directors
Information
Note 2
Note 1
Transportation: - CITO - Security Authority
Finance: SAP CCC
CSU Infrastructure Managers
CSU Business Solutions Managers
Corporate Information Management
Corporate Enterprise Architecture
SAP Projects Office
Corporate Policies & Strategies

Note 1
- Some Directors of IT may report directly to Deputy Ministers
- Some report directly to Executive Directors of Information Management within departments
- Some report to other Executive Directors within Departments
- Some Directors of IT serve single departments while others serve multiple departments and agencies

Note 2
- These organizations provide corporate-wide IT services but report within their home departments only

3.17 Although the corporate organizational structure for IT is still confusing and somewhat onerous, we view the creation of the CIO role as an important step in establishing an effective governance framework for information technology.

3.18 *Significant centralization project* – A proposal for a significant reorganization of certain IT functions has been submitted to Executive Council. It focuses on combining Corporate IT Operations, and the IT operation and support services of the corporate service units, to create a new IT infrastructure service management organization reporting to the Chief Information Officer. This initiative has been under development for over four years and awaits Executive Council approval. Corporate IT Operations indicated there have been staffing challenges over the past few years due to the uncertainty of whether this reorganization will take place. If approved, this initiative will go far in standardizing the IT service delivery role in government and will significantly refocus the corporate IT organizational structure. It will also have a significant impact on IT security as the new, centralized service delivery function will be responsible for many security-related matters.

Recommendation 3.1
A decision on the proposal to reorganize and centralize IT service delivery should be made by Executive Council as soon as possible.

GOVERNMENT-WIDE: INFORMATION TECHNOLOGY SECURITY

3.19 *Unclear lines of authority* – A critical requirement of a well-functioning governance framework is that those responsible for an operational area have the authority needed to effectively perform their responsibilities. We identified situations in government's corporate IT operations in which this is not the case.

3.20 The lack of an organizational structure with clear lines of authority has led to a deficiency in the oversight of a significant IT security initiative. A secure identity management (SIM) project was undertaken to improve security over the management of user access privileges for government information systems. Upon implementation, the new system provides users with one login code and password for all the computer systems they require to carry out their assigned responsibilities. This will help ensure that when new users are set up for a computer system, they are provided only the access privileges they need and these privileges are compatible. When an employee transfers to another department or leaves government, their access can be quickly changed or removed for all the computer systems they used.

3.21 The SIM project was implemented by Corporate IT Operations. It was agreed that corporate service units (CSUs) would have the new process completely established for their client departments by April 1, 2008. Some CSUs embraced this new process quickly and set up their client departments' computer users in the system. However, as of February 2009, other CSUs are still not using SIM or are very slow in making progress. We believe insufficient action has been taken to compel complete and timely participation. As a result, user access privileges may not be managed on a consistent basis and efficiencies from this new process will not be fully realized. The greater risk of errors or lack of timely changes or cancellations of user access associated with the old way of doing things will remain.

Recommendation 3.2
All corporate service units should be required to participate in the secure identity management project and take the steps necessary to fully implement the new system as soon as practical.

3.22 The Corporate Information Strategies Division is another example of unclear lines of authority. This Division is responsible for developing and implementing government information management and information technology policies and standards. Although the expectation is that such IT policies are to be complied with by all departments and agencies, the current organizational framework for IT operations provides little authority to enforce compliance. A third example of unclear lines of authority concerns the requirement for reporting computer virus infections to Corporate IT Operations and the Security Authority. Such reporting is not enforced and management informed us that it sometimes does not occur.

GOVERNMENT-WIDE: INFORMATION TECHNOLOGY SECURITY

Recommendation 3.3
The organizational framework for government's IT operations should ensure there is adequate authority for the enforcement of significant government-wide IT policies and standards.

3.23 *Security Authority* – The Wide Area Network (WAN) Security Policy establishes specific roles for oversight and management of the security of the corporate network. One of the key roles is that of the Security Authority, a management-level position within the Department of Transportation and Infrastructure Renewal which reports to the Executive Director of Public Works. The position's responsibilities include directing the implementation of the WAN security policy, and managing and monitoring the corporate network, including the responsibility to approve all IT devices and applications connecting to the network.

3.24 The Security Authority is also assigned certain audit responsibilities focused on ensuring ongoing compliance with the policy and its related standards. However, Corporate IT Operations also reports to the same Executive Director as the Security Authority. This could result in the Security Authority having to audit and report upon directives given, or approved by, the person to whom he reports. We believe the Security Authority requires a greater degree of independence from the entity that it monitors and audits than afforded under the existing structure.

Recommendation 3.4
Government's organizational framework for IT operations should have the Security Authority and Corporate IT Operations reporting to different positions in the organization.

3.25 The Security Authority's audit responsibilities relate to 17 aspects of WAN security. Since its establishment in 2004, the Security Authority has been a one-person role. This resulted in very limited ability, from a resource perspective, to perform the audit function, other than on an exception basis. Having only one person to monitor and enforce a WAN security policy and associated standards in an organization as large as the Nova Scotia government is not effective. As a result, WAN security may not be adequately monitored on a timely basis. There is also higher risk of vulnerabilities not being detected, resulting in security incidents occurring (e.g., computer viruses, hacking attempts). We believe either the Security Authority role needs more staff or some of its responsibilities need to be reassigned.

Recommendation 3.5
The role and responsibilities of the Security Authority should be reviewed to determine the resources required to effectively perform security monitoring and auditing functions, and where best those responsibilities and resources should be assigned.

Planning for Information Technology Security

Conclusions and Summary of Observations

Planning for information technology security is not adequate. We identified the need for an IT security oversight committee, corporate IT security charter and corporate IT security plan. There is also a need for corporate data classification standards.

3.26 *IT security planning* – There is no single group in the Nova Scotia government responsible for the planning of IT security. Planning for information technology security should begin with an executive oversight group, tasked with strategic-level responsibility for security planning, policy setting, risk management, IT resource management and IT performance management. A properly focused IT security oversight group would draw its mandate from the IT governance framework. It would have representation from key functional areas which impact on government-wide IT security, such as information management, IT operations, IT security, internal audit, human resources and legal services. The oversight group will work to ensure government's IT operations are aligned with its business objectives (e.g. a government program managing personal information is supported by a sufficiently secured computer system). The group also has a significant role in defining roles, responsibilities and authorities surrounding IT security, and in ensuring important security measures are in place.

Recommendation 3.6
A government-wide IT security oversight group should be established, and given responsibility for security planning, policy setting, risk management, IT resource management and IT performance management. The group should include representation from government functions with a role to play in IT security, such as information management, IT operations, IT security, internal audit, human resources and legal services.

3.27 We also determined government does not have a corporate security charter. A security charter can be used to define the amount of risk the organization is willing to bear. Based on this level of risk, the charter can address the objectives, responsibilities and accountabilities of the IT security management function. The absence of a well-defined security charter, or similar analysis, could lead to misaligned IT and business objectives, as well as a deficiency in the implementation and oversight of IT security.

Recommendation 3.7
A security charter should be developed to address the scope of government-wide IT security, and the objectives, responsibilities and accountabilities of the IT security management function.

3.28 Neither government, nor any of its corporate service units, has an IT security plan. Large organizations need a plan to ensure that IT security is properly focused, designed and managed. The purpose of the plan is to provide a strategic framework for identifying key business processes, associated security risks, and measures required to mitigate significant risks identified.

3.29 An IT security plan will take into consideration the nature of the IT infrastructure employed, as well as the financial, human and other resources available to manage IT security. The plan must be updated as IT and its related risks evolve. The risks of not having an IT security plan include: IT security activities not being aligned with its business strategy; inefficiencies due to redundant security measures or equipment; heightened exposure to security threats such as viruses and unauthorized computer access; and security measures compromised by a lack of standards or failure to comply with standards.

Recommendation 3.8
A corporate IT security plan should be developed and implemented.

3.30 *Data Classification Standards* – The government of Nova Scotia has adopted national data classification standards, but has not yet applied them to most of its information holdings. Data classification standards are used to guide the protection of information collected. They identify the sensitivity and value of different types of information so that IT security can be focused where it is most needed. For example, personal information relating to members of the public would normally be classified as highly confidential and requiring high security; whereas demographic statistics which are routinely available upon request may require less security.

GOVERNMENT-WIDE: INFORMATION TECHNOLOGY SECURITY

3.31 Data held in large government and corporate databases can be very valuable to the criminal element as a means of conducting unlawful activities such as identity theft, stealing of credit card information, and sending out mass-mailings enticing recipients to enter into fraudulent schemes. Data classification standards help ensure IT managers and other users are aware of the level of protection appropriate for the specific information they are maintaining. Without such standards, sensitive information could be inadequately protected, or inappropriately disclosed.

Recommendation 3.9
Data classification standards should be implemented for all of government's information holdings.

IT Security Policies and Standards

Conclusions and Summary of Observations

Government's current security policies and standards need to be strengthened. There is no government-wide acceptable use policy, the threat risk assessment process guide is out of date, and laptop security guidelines do not address the securing of all mobile computing devices and lack the authority of policy. We also observed instances where government IT security policies were not complied with. There were an insufficient number of threat risk assessments performed and inadequate security training for computer users.

3.32 *Policies and standards* – The government of Nova Scotia has a number of information management and information technology policies, standards and guidelines related to security; which include the following.

- Information Management Policy
- Wide Area Network Security Policy
- Wide Area Network Security Standards
- Wide Area Network Security Processes
- Electronic Mail Policy

- Citizen Online Identity Authentication Policy
- Website Privacy Policy
- WAN Threat Risk Assessment Process Guide
- Laptop security guidelines

We noted that some corporate service units also have security policies and guidelines.

3.33 We were encouraged to see that government has established and implemented the above noted policies, standards and guidelines. The Information Management Policy, which became effective on October 1, 2008, is perhaps the most important of the policies. It addresses the collection, use, and management of information by government, regardless of where and how the information is collected or maintained. It is viewed as the lead policy because all of the IT-related policies, standards and guidelines draw their purpose and authority from it. These policies, as a package, partially set the stage to define an effective management and control framework around IT operations, and IT security. However, we observed certain issues related to government's IT policies and standards.

3.34 Nova Scotia Economic and Rural Development's Corporate Information Strategies Division is responsible for all corporate IT policies. The Wide Area Network (WAN) Security Policy was approved April 1, 2002 and has been effective since April 1, 2003. The policy is not included in government's management manuals, although it is listed in the table of contents of Manual 300. However, the policy is available on the government's intranet site. Management Manual 300 is where government employees expect to find government operational policies. If the WAN security policy is not in this manual, some government staff may not be aware of the policy, or know where to find it.

Recommendation 3.10
The Wide Area Network Security Policy should be published in Management Manual 300.

3.35 *Threat risk assessments* – The government has a WAN Threat Risk Assessment Process Guide to aid in recognizing and addressing vulnerabilities in the Wide Area Network. This guide has been in place since 1998, and states that it should be updated annually, or whenever an occurrence reveals a deficiency in the existing guidelines. However, there is no indication that the guide has been reviewed for updating in the last ten years. The implication of not updating the guide is that it will quickly become out of date as technology-related practices change and new practices are developed.

Recommendation 3.11
The Wide Area Network Threat Risk Assessment Process Guide should be reviewed and updated annually to ensure it is consistent with current standards and continues to meet the changing needs of government.

3.36 We are aware of two threat risk assessments performed in the past year which addressed the provincial data centre and the major business applications of one department. However, we were informed that it has been more than ten years since the last threat risk assessment was conducted for the government wide area network, and most CSUs have not conducted such assessments. Without a comprehensive threat risk assessment of the entire corporate network, there is no assurance that IT security around the government network is adequately planned, managed and performed, or that security measures meet the needs of the departments which own the systems.

GOVERNMENT-WIDE: INFORMATION TECHNOLOGY SECURITY

Recommendation 3.12
A detailed threat risk assessment should be performed on the wide area network. In addition, all CSUs should perform threat risk assessments on the infrastructure and applications for which they are responsible. These assessments should be updated on an annual basis, or sooner if significant changes occur.

3.37 *Acceptable use policy* – The Nova Scotia government began drafting an acceptable use policy and guidelines in June 2007 to convey to employees and contractors the specifics of acceptable use of corporate IT systems. For example, it is unacceptable for an employee to use government computers for operating a personal business and contractors should only use systems for purposes related to their contract assignment. However, the government's acceptable use policy and guidelines are still in draft form, and there is no indication of when they will be completed and approved. Some CSUs developed their own acceptable use standards based on the draft corporate document. Without government-wide standards to guide government employees and contractors in the acceptable uses of IT resources, government systems may be burdened by personal or inappropriate use, or used for unlawful or unethical purposes.

Recommendation 3.13
The corporate acceptable use policy and guidelines should be completed, approved and effectively communicated to all government employees and contractors.

3.38 *Security awareness* – The WAN Security Standards indicate that there will be a corporate network IT security awareness program and that basic security awareness training will be provided to all employees on a regular basis.

3.39 At the time of our audit there was no formal IT security awareness training available for government employees. The provision of security awareness training is the responsibility of the Security Authority and the Client Security Officers of each CSU. The Security Authority developed security awareness presentations and delivered these to the Client Security Officers, as well as small groups around government from time to time. However, the Client Security Officers have not delivered such training to the staff of their CSUs or client departments. The Security Authority indicated that the primary issue is the lack of funds budgeted to develop and deliver a corporate IT security awareness program.

3.40 The implication of this is users are not aware of security requirements associated with their use of government computers. For example, without IT security awareness training, users may be vulnerable to social engineering attacks. These attacks may come in the form of email or phone calls from persons falsely claiming to be government IT operators. The illicit calls may request sensitive information such as user identification codes and passwords, or confidential government information available to the employee.

Recommendation 3.14
An IT security awareness strategy should be developed and implemented to address all government employees who have access to important government systems and information.

3.41 *Security certification and accreditation* – The WAN Security Policy also states *"IT system security certification and accreditation shall be performed on the Corporate Network (including all hardware and software that comprises the Corporate Network) throughout the planning, implementation, and operations life cycle."* The policy document, which came into effect in 2003, indicates this specific directive is not in force at this time. Management informed us that security measures are not yet strong enough to ensure successful achievement of certifications and accreditations.

Recommendation 3.15
The directive requiring security certifications and accreditations for IT systems should be reviewed to determine whether it should be in force at this time. If the review determines that the directive will be put in force at a later date, a plan should be prepared with a timeline of required changes which must first be made.

3.42 *Independant security assessments* – Best practices indicate that large organizations should have periodic independent security assessments. Such assessments provide assurance that critical IT systems are adequately designed, managed and operated, with appropriate controls in place. We found there is no provision in the WAN Security Policy that requires periodic independent security assessments, and no such assessments have been performed on the government WAN. The government has an annual audit performed on its financial reporting systems to support various financial statement audits, but these audits do not address all critical government systems and all security-related matters. As a result, it is possible there could be weaknesses or vulnerabilities that have not been detected which could pose a threat to the security of government's IT systems.

Recommendation 3.16
The Wide Area Network Security Policy should be amended to require periodic independent assessments of wide area network security.

3.43 *Security screening* – Some CSUs complete security screening when hiring IT staff, such as checking employment references, character references, criminal record checks and child abuse registry checks. Other CSUs do not go beyond basic employment reference checks. IT staff, due to the nature of their responsibilities for maintaining IT systems, often have access to very sensitive information and have powerful computer operating abilities. The risk of IT security being compromised from within government is increased when thorough background checks are not performed on all new IT staff.

Recommendation 3.17
The hiring process for IT employees should include criminal record checks and child abuse registry checks.

3.44 *Mobile computing devices* – The government has many mobile computing devices deployed to its employees. These include laptop computers, BlackBerries and other smartphones. These devices often contain confidential information and, because of their portability, are subject to increased risk of theft or loss. The government has laptop security guidelines which briefly refer to other mobile devices. These guidelines provide advice concerning the importance of using firewalls, anti-virus software and updating operating systems. The guidelines also focus on physical protection and note steps that should be taken to protect such devices from damage or theft. However, the guidelines are silent with respect to the importance of using passwords or encrypting data contained on the devices.

3.45 Since laptop computer security is addressed by guidelines, employees are expected to be aware of and follow them, but are not formally compelled to comply with guidelines. We feel there should be specific policy or standards around the security guidelines of mobile devices, with emphasis on the requirement to make passwords mandatory. Many Deputy Ministers and senior officials use BlackBerries which generally contain emails received and sent. We do not know how many of these devices are password protected, but if an unsecured one was lost, any confidential information contained on it could be quickly accessed and potentially made public.

Recommendation 3.18
Laptop security guidelines should be reviewed and updated to address all security issues surrounding mobile computing devices. Further, the new document should be approved, implemented and communicated in the form of a policy or set of standards.

Monitoring and Enforcing Compliance

Conclusions and Summary of Observations

Management practices for monitoring and enforcing compliance with policies and standards are not adequate. Areas for improvement include more attention to the costs and benefits of network monitoring devices, the formalization of government's computer emergency response team, and better security over the use of wireless internet access.

3.46 *Monitoring and enforcement of policies and standards* – We noted very little monitoring of security logs for the wide area network, other than on an exception basis where something unusual occurred. In those instances the logs were reviewed after the fact to try and determine the cause. An important IT security strategy is to have security devices (e.g., firewalls) built into a computer network to prevent or detect, and promptly report, successful or unsuccessful attempts to breach system security. However, to maximize their effectiveness, the devices' security logs need to be monitored for known patterns or other characteristics of security incidents.

3.47 There are many logs produced by security devices on the government network. We were informed that there is insufficient staff available to monitor these logs, even with the use of specialized monitoring software. The implication of this is that security weaknesses could be exploited without the knowledge of those operating and managing the network.

3.48 Further, we were informed that funds have been made available for security devices but they have not been acquired because there was no staff available to manage and monitor them.

Recommendation 3.19
A review should be performed to determine the nature and extent of security devices required to provide adequate protection to the wide area network, along with an estimate of the financial and human resources required to implement and manage them.

3.49 Many large organizations have a computer emergency response team (CERT) to take the lead in responding to significant security incidents or emergencies if they occur. Such a team is vitally important to provide an organized and rapid response to events that can significantly harm government IT systems and the operations they support. The CERT should have representation from all major areas of the business and have a well-defined mandate.

GOVERNMENT-WIDE: INFORMATION TECHNOLOGY SECURITY

3.50 The government has an informal CERT in place. A detailed CERT framework was developed in 2004 which outlined the mission, purpose and membership of the group. However, this framework document has not been kept up-to-date. Our interviews indicated that the CERT has no formal meetings, and there is only general awareness of its existence and function. CSUs know that in the event of a security incident they are to report immediately to the Security Authority and he will determine what action is required.

3.51 We were informed that the CERT is comprised of IT staff only. As a result, emergency responses relating to incident handling, vendor relations, communications, legal and criminal investigative issues may not be adequately addressed. We are also concerned whether the CERT will notify the CSUs and departments on a timely basis of the need to enact their business continuity and disaster recovery plans if a significant security event occurs.

Recommendation 3.20
The CERT framework of 2004 should be reviewed and updated, and a plan developed to formally implement an effective team that is properly trained to respond to serious security incidents as soon as they are detected.

3.52 Wireless communication enables ease of connecting to a computer system from any location within range or a wireless access point (e.g., a wireless router). Wireless access also provides a means for unauthorized persons to connect to a system if a wireless access point is unsecured or the access codes are known.

3.53 During the planning stage of this audit we found information on the government intranet, a network accessible only by Nova Scotia government employees, which openly provided the access codes for one of government's wireless access points. This wireless access point was not connected to the government WAN and the service was provided solely to assist visitors to a department who needed internet access (e.g., for purposes of making presentations). However, there are over 10,000 government employees, as well as many contractors, who have access to the government intranet. Providing access codes on the intranet could lead to someone using this connection to the internet (e.g., while sitting in a car outside of the building housing the connection) for inappropriate or unlawful purposes.

GOVERNMENT-WIDE: INFORMATION TECHNOLOGY SECURITY

Recommendation 3.21
Access codes for wireless internet connections should not be disclosed to individuals who have no cause to use the connection.

Response: Treasury and Policy Board

RESPONSE: TREASURY AND POLICY BOARD

Treasury and Policy Board would like to thank the Auditor General for the opportunity to respond to the report of government-wide audit of Information Technology Security.

Like many organizations, the government's use of and dependence on Information Management/Information Technology (IM/IT) has increased. IM/IT is recognized as a prominent and strategic government business enabler as evidenced by current directions such as e-service delivery, shared services, and horizontal government as well as the appointment of a Chief Information Officer in December, 2008.

The Information Management/Information Technology community understands the critical importance of security and how it impacts responsible and effective management of governments information and technology assets. The province has adopted an IM/IT vision. The three major components of that vision include Quality and Accessibility of Government Services, Sustainable Operation of Government, and Optimal Use of Information. All components of this vision respect the privacy, accessibility, and security requirements for personal and confidential information.

The Information Management Strategy and Framework, approved by the Deputy Ministers in December, 2005, highlighted the importance of security with regard to government's information assets. In fact, protection is one of the Information Management Framework's six principles. The strategy recommends the creation of an IM Policy and an associated Information Management Requirements Analysis (IMRA) Tool. These were developed by the Corporate IM Program and came into affect on October 1, 2008 providing a consistent method for departments to assess their programs, services, and IT systems for compliance with IM requirements including security. The IMRA contains a section dedicated to the protection principle to help ensure existing security and privacy requirements are addressed.

The basic elements of corporate IT security are in place, as are an Information Management Policy, Wide Area Network Security Policy, Security Standards and Processes as well as various other corporate and departmental security-related policies and guidelines. This strong foundation has enabled government to protect its information assets against unavailability, loss or misuse.

While our current IT Security program has enabled us to achieve good results we recognize security is an ongoing matter that must be planned for, continually monitored, and managed to keep ahead of new and emerging threats.

Current initiatives, in Nova Scotia, include the development of an IT Strategic Plan, IM/IT Governance Framework, Enterprise Architecture, and Business

Intelligence Strategy as well as the continued implementation of the Information Management Strategy. These projects will continue to persistently incorporate and address privacy and security considerations including planning, monitoring, enforcement, and policy/standard development.

RESPONSE: TREASURY AND POLICY BOARD

The Auditor General's twenty-one recommendations are accepted in principle. While I believe plans currently in place to address the IT Governance issues raised in the Auditor General's report of February 2008, and plans to restructure IT Services Delivery in the province, will address most of the recommendations, the results of the audit will be forwarded to the Business Technology Advisory Committee (BTAC), a Deputy Minister sub-committee of Treasury and Policy Board, for their review and follow-up. The Chief Information Officer will ensure that an investigation of these recommendations occur in order to provide advice to BTAC as they determine next steps.