AUDIT OF IT SECURITY

Corporate Internal Audit Division
Natural Sciences and Engineering Research Council of Canada
Social Sciences and Humanities Research Council of Canada
September 20, 2012

Table of Contents

1 Executive Summary

1.1 Introduction

Natural Sciences and Engineering Research Council of Canada (NSERC) and the Social Sciences and Humanities Research Council of Canada (SSHRC) (the Agencies) are two federal government agencies supported by a Common Administrative Services Directorate (CASD), which manages Information Technology (IT) and IT security for both Agencies. The Agencies are subject to the Treasury Board Policy on Government Security (PGS) and to its supporting directives, standards and guidelines which require that information, assets and services are protected against compromise.

An audit of the Agencies' IT security was conducted because:

- IT security was identified in the 2011-14 Internal Audit Risk-Based Audit Plan (RBAP) as an area meriting further examination;
- TBS' Management of IT Security (MITS) requires that IT security be part of the RBAP;
- An audit of IT security has not been conducted in the Agencies in the last 10 years; and
- The consequences of an IT security breach to the Agencies could be severe.

The subject of this audit is the Agencies' joint IT security program. The audit examined the state of the IT security program and related activities between April 1, 2011, and the end of December 2011. The audit started with a high-level assessment of IT security and a related risk assessment, which were used to formulate an audit plan focusing on the program elements of higher audit priority.

1.2 Background

Information is often viewed as a critical component or asset to most if not all organizations because most of them cannot function if this element is not available or is unreliable. In today's world, availability, integrity and confidentiality of information are paramount concerns, and for that reason, the Agencies are subject to the Policy on Government Security (PGS) and its supporting directives, standards and guidelines.

As the Agencies are handling and will continue to handle more and more of their business electronically, it is clear that they have made great strides in strengthening competencies around IT security. For example, IT security policies have recently been drafted, and automated tools were purchased and implemented to continually enhance and protect the Agencies' systems from vulnerabilities. It will be important for the Agencies to continue this momentum of continuous improvement in IT security into the future. This report provides additional recommendations in that regard.

1.3 Objectives and Scope

The objectives of this internal audit assignment were to assess and report on the effectiveness of selected NSERC and SSHRC IT security controls. Specifically, this audit

provides assurance on the adequacy and effectiveness of the Agencies' main IT security controls in the following areas:

- IT security program governance;
- IT security program framework;
- boundary and perimeter defence;
- logical access controls and privileged access to systems (i.e. awards management systems);
- change and configuration management processes;
- vulnerability management; and
- physical security of the server room.

1.4 Identified Strengths

A number of activities related to the IT security program were evident during the audit as a result of the Agencies' increased emphasis on IT security. Some IT security strengths included:

- Drafting of an IT security policy and directive among other security documentation improvements;
- Establishing a Departmental Security Officer (DSO);
- Conducting independent security reviews during the audit period, including an ITSS Independent Security Assessment in April 2011 and a Departmental Asset Protection and Security Assessment in December 2011;
- Making significant improvements to patch management;
- Establishing a formal Change Control Board;
- Having an established policy in place which requires approval by the IT Security Coordinator for changes that could compromise security;
- Having security architecture and secure remote access in place that include a perimeter firewall configured with several zones, a remote access service (VPN) that requires two-factor authentication to gain access, and a network intrusion detection system. In addition, implementation of a newer, more secure remote access solution was underway during the audit period;
- Having formally documented procedures for Network, Remote Access NAMIS/AMIS[1] application user administration; and
- Having passwords on some systems that were in line with leading practices.

[1] NAMIS is the NSERC Awards Management Information System and AMIS is SSHRCs Awards Management Information System.

1.5 Key Audit Findings

While the Agencies have had a recent focus on IT security, the audit identified some areas where further IT security improvements are recommended:

IT Security Program Governance

The Departmental Security Officer and IT Security Coordinator positions have been established; however, there is no identified senior oversight committee or senior board that regularly reviews the state and performance of the IT security program. An NSERC-SSHRC IT Security Plan, which is a Treasury Board requirement, has not been developed.

IT Security Program Framework

It was noted that an IT Security Policy and some supporting documentation have been drafted but these have been not approved by management or communicated to staff. It was further noted that an overall framework that defines the components of the IT security program is not in place. Supporting procedures, directives or standards have not been defined. Supporting procedures, directives and standards are informal or not in place.

Formal IT Security Processes and Procedures

It was noted that in many areas, including boundary and perimeter defence, access control, change and configuration management, there are informal processes and procedures in place.

The Agencies have some formally documented procedures in place such as the Network, Remote Access NAMIS/AMIS application user administration. In cases where formal procedures are in place, and internal controls have been implemented, it was noted that evidence to confirm that procedures are followed is not always retained. Without sufficient audit trail documentation, it is difficult to determine whether controls are operating as intended.

Access controls

Opportunities for improvement were noted in the area of access control. Processes for user administration are informal for some systems. In other cases, formal procedures have been documented but it was noted that they were not followed consistently. Sample-based testing found examples of inadequate documentation to support the approval for access that was granted to users, including privileged users, and accounts belonging to terminated employees that were not removed in a timely manner. Shared administrator accounts were also found to be in use. Furthermore, there is no formal password standard at the Agencies. As a result, password strength (minimum length, complexity, expiry, etc.) varied across systems. Some systems had password settings that were in line with leading practices, while some were not. In addition to logical access, opportunities for improvement were noted in physical access controls over the server room.

Vulnerability Management Program

It was noted that significant improvements have recently been made with regards to infrastructure patch management, including the implementation of an automated patch management tool. It was also noted that an informal

vulnerability management program is in place; however, a critical cyber alert was not followed through, in part due to a lack of communication between security staff and other supporting IT management. In addition, no evidence could be provided to determine whether or not specific cyber warnings had been addressed. An internal technical vulnerability testing program had not been exercised during the audit period nor was there any evidence of related procedures, findings or corrective action taken.

1.6 Recommendations

1. It is recommended that the Agencies re-examine the IT security program governance structure and include senior management oversight of the program under the mandate of one of the existing senior committees/governance bodies to carry out the regular reviews of IT security priorities, plans and performance and to communicate the importance of the function to the organization. Furthermore, it is recommended that a departmental security plan be developed as required by the Treasury Board Directive on Departmental Security Management, and include regular reviews of the IT security program.
2. It is recommended that the IT Security Policy be finalized, approved and communicated to all employees, as intended by management. In addition, it is recommended that the Agencies undertake a thorough review of its IT security framework. This includes the IT Security Policy, directives, standards, guidelines and the processes and procedures needed to implement them within the Agencies' operational context. This review should be conducted within the context of the latest Treasury Board and Lead Security Agency policy, directives, standards and guidelines and should ensure that security control objectives and controls, as well as risk management are integrated into the Agencies' IT security program.
3. It is recommended that the Agencies formalize their security and change management processes and develop procedural documentation to support operations to ensure that processes and procedures are followed consistently. Furthermore, it is recommended that documentation of key controls (e.g. approvals, security reviews, change management documentation, etc.) be retained for audit trail purposes.
4. It is recommended that all user administration procedures, including those for physical access, be formalized, and existing procedures be communicated to staff to ensure they are followed consistently. User administration procedures should include a requirement for periodic review of all accounts, and document the use of administrator and privileged accounts. Furthermore, a password standard should be defined in line with leading practices, and existing passwords should be reviewed and brought into line with this standard. A procedure for monitoring of physical access to the server room should be developed and implemented.
5. It is recommended that the vulnerability management process be reviewed and brought into line with leading practices, including the process for escalation and communication of vulnerabilities and documenting risk management decisions. The technical vulnerability testing process should also be reviewed, formalized and applied on a regular basis. Evidence of vulnerability testing and follow-up on identified vulnerabilities should be retained for audit trail purposes. In addition, it

is recommended that the patch management process be reviewed, formalized and extended to all network components and application systems

1.7 Conclusion

There is a current focus on IT security and a number of improvements to the IT security program are currently underway at the Agencies. Nevertheless, it must be emphasized that the program requires critical governance elements, a complete policy and managerial framework and requires that informal processes and procedures be formalized and documented to reduce the risk of breaches to IT security.

2 About the Audit

2.1 Background

An audit of the Agencies' IT security was conducted because:

- IT security was identified in the 2011–14 Internal Audit Risk-Based Audit Plan as an area meriting further examination;
- TBS' Management of IT Security (MITS) requires that IT security be part of the RBAP;
- An audit of IT security has not occurred in the Agencies in the last 10 years; and
- The consequences of an IT security breach to the Agencies could be severe.

The Agencies are subject to the Policy on Government Security (PGS) and to its supporting directives, standards and guidelines. The PGS requires that information, assets and services are protected against compromise and that individuals are protected against workplace violence.

Under the PGS and its supporting direction and guidance, security management requires the continuous assessment of risks and the implementation, monitoring and maintenance of appropriate internal management controls involving prevention (mitigation), detection, response and recovery. The management of security intersects with other management functions including access to information, privacy, risk management, emergency and business continuity management, human resources, occupational health and safety, real property, materiel management, information management, information technology (IT) and finance. Security is achieved when it is supported by senior management, an integral component of strategic and operational planning, and embedded into departmental frameworks, culture, day-to-day operations and employee behaviours.

The PGS suite includes key "must do" documents such as the Directive on Departmental Security Management (2009) and the Treasury Board's Management of Information Technology Security (MITS) standard among other federal government directives, standards and guidelines.

The Directive on Department Security Management defines the roles and responsibilities of departmental employees who support deputy heads in the management of departmental security. These responsibilities form the basis for effective decision making and accountability related to departmental security activities. This directive also establishes the minimum security control objectives that a department must achieve to ensure that its mandate, operations, priorities and security requirements are met.

IT security is, without doubt, emerging as one of the most important elements in IT planning and implementation. As the Agencies are handling and will continue to handle more and more of their business electronically, it is clear that the Agencies have been focussing on strengthening competencies around IT security, which was made evident at the beginning of this audit. For example, IT security policies have recently been drafted, and some automated tools were purchased and implemented to help protect the

Agencies' systems from vulnerabilities. It will be important for the Agencies to continue this momentum of continuous improvement into the future.

2.2 Objective and Scope

The objectives of this internal audit assignment were to examine, assess and report on the effectiveness of selected NSERC-SSHRC's IT security controls. Specifically, this audit provides assurance on the adequacy and effectiveness of the Agencies' main IT security controls in the following areas:

- IT security program governance;
- IT security program framework;
- boundary and perimeter defence;
- logical access controls and privileged access to systems (i.e. awards management systems);
- change and configuration management processes;
- vulnerability management; and
- physical security of the server room.

2.3 Methodology

The approach and methodology used for this audit is consistent with the Internal Audit Standards as outlined by the Institute of Internal Auditors (IIA), and is aligned with the Internal Audit Policy for the Government of Canada.

The audit commenced with a survey phase, where preliminary interviews were conducted and documentation was reviewed in order to understand the current state of IT security risk and control. Coming out of the survey phase was an IT security risk assessment.

The audit program, including detailed audit criteria and procedures, were then designed based on this understanding and focussed on the seven key areas defined above.

Besides the MITS Standard, the development of audit criteria also considered industry standards, including ISO 27002. ISO 27002 is a code of practice for information security which establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management within an organization. The standard also provides guidance for the development of organizational security standards and effective security management practices.

The following methods were used to gather audit evidence:

- Conducting interviews and reviewing documentation;
- Identifying key internal controls and reviewing security processes and standard operating procedures;
- Performing walk-throughs of key controls and processes; and
- Testing of the operating effectiveness of controls via inquiry, supported by observation and/or examination of documentation.

The application of these procedures allowed the formulation of a conclusion as to whether the audit criteria were met, partially met or not met. Evidence was gathered in compliance with Treasury Board policy, directives, and standards on internal audit, and the procedures used were in line with the professional standards of the Institute of Internal Auditors. Information was assessed for sufficiency, reliability, relevance and usefulness, and conclusions were drawn as to whether documented evidence met the objectives of the audit.

3 Observations and Recommendations

3.1 Areas of Strength

A number of activities related to the IT security program took place during the audit as a result of the Agencies' increased emphasis on IT security. Strengths included:

- Drafting of an IT security policy and directive among other security documentation improvements;
- Establishing a Departmental Security Officer (DSO);
- Conducting independent security reviews during the audit period, including an ITSS Independent Security Assessment in April 2011 and a Departmental Asset Protection and Security Assessment in December 2011;
- Making significant improvements to patch management;
- Establishing a formal Change Control Board;
- Having an established policy in place which requires approval by the IT Security Coordinator for changes that could compromise security;
- Having security architecture and secure remote access in place that include a perimeter firewall configured with several zones, a remote access service (VPN) that requires two-factor authentication to gain access, and a network intrusion detection system. In addition, implementation of a newer, more secure remote access solution was underway during the audit period;
- Having formally documented procedures for Network, Remote Access NAMIS/AMIS application user administration; and
- Having passwords on some systems that were in line with leading practices.

3.2 Areas of Improvement

3.2.1 IT Security Program Governance

In order to effectively manage security risks, a governance structure for IT security must be established and have clear mandates and oversight of IT security, including the review of priorities, plans and performance of IT security. In addition, the Treasury Board Secretariat (TBS) Directive on Departmental Security Management requires the development of a departmental security plan.

It was noted that an IT security coordinator and a Departmental security officer have been named in draft security documents; however, there is no senior management oversight body that meets regularly and reviews information related to IT security priorities and plans, provides advice on issues, reviews performance of the IT security function, and communicates its decisions to the organization in a timely manner. While several senior management committees exist, including an IM-IT Bi-Council Steering Committee, none have responsibility for IT security included in their terms of reference. While the development of a departmental security plan is mentioned in a draft asset protection and security priorities document, the plan has not been developed. In addition, while some IT security review work has been undertaken (the most recent being a threat risk assessment that remains in draft form), there is no formal process in place to determine what types of reviews should be conducted and at what intervals.

Recommendation: It is recommended that the Agencies re-examine the IT security program governance structure and include senior management oversight of the IT security program under the mandate of one of the existing senior committees/governance bodies to carry out the regular reviews of IT security priorities, plans and performance and to communicate the importance of the function to the organization. Furthermore, it is recommended that a departmental security plan be developed as required by the Treasury Board Directive on Departmental Security Management, and that it include regular reviews of the IT security program.

3.2.2 IT Security Framework

A complete IT security framework includes a defined, approved IT security policy that is supported by key procedures, standards and directives and adheres to TBS policy. The Agencies have an draft IT Security Policy, but it has not been approved by management or been communicated to all employees. The draft Policy does not include a framework for establishing IT security control objectives and controls or risk management. In addition, limited supporting procedures, directives or standards have been defined. In particular, supporting processes and procedures required to support the MITS standard tend to be informal and/or not documented. There are opportunities to improve security education, training or awareness requirements, business continuity management, consequences of information security policy violations, and definition of roles and responsibilities, including reporting security incidents.

Recommendation: It is recommended that IT Security Policy be finalized, approved and communicated to all employees, as intended by management. In addition, it is recommended that the Agencies undertake a thorough review of their IT security framework. This includes the IT security policy, directives, standards, guidelines and the processes and procedures needed to implement them within the Agencies' operational context. This review should be conducted within the context of the latest Treasury Board and Lead Security Agency policy, directives, standards and guidelines and should ensure that security control objectives and controls as well as risk management are integrated into the Agencies' IT security program.

3.2.3 Formal IT Security Processes and Procedures

Formal documented processes and procedures are a key component of IT security to help ensure that processes are followed consistently and security risks are addressed. It was noted that in many areas of IT security there are only informal processes and procedures in place, including:

- The process for establishing and maintaining boundary/perimeter zones to maintain security;
- The process for reviewing and approving the security impact of infrastructure changes;
- The procedures and checklists for administration of key security components such as firewalls;
- The infrastructure hardening guidelines; and
- The process for technical vulnerability testing.

The limited formal, documented processes and procedures increase the risk of managerial errors or omissions that have the potential to compromise IT security.

The Agencies do have some formally documented procedures in place, including the Network, Remote Access NAMIS/AMIS application user administration. In cases where formal procedures are in place and internal controls have been implemented, it was noted that evidence to confirm that procedures are followed is not always retained. Examples noted during the audit include:

- A policy is in place that requires approval by the IT Security Coordinator for changes that could compromise security; however, evidence of security reviews or approvals by the IT Security Coordinator for a sample of infrastructure and application changes could not be provided;
- Formal procedures for account creation are in place for the network and some applications; however, for a sample of new accounts, evidence of approval could not be provided; and
- Some technical vulnerability testing is conducted; however, no evidence of the testing and corrective action taken could be provided.

Without sufficient audit trail documentation, it is difficult to determine whether controls are operating as intended.

Recommendation: It is recommended that the Agencies formalize their security and change management processes and develop procedural documentation to support operations to ensure that processes and procedures are followed consistently. Furthermore, it is recommended that documentation of key controls (e.g. approvals, security reviews, change management documentation, etc.) be retained for audit trail purposes.

3.2.4 Access Controls

Key components of effective logical access control include a formal authorization process for assigning and removing access to systems, regular review of user access to systems, control over administrative accounts, and strong password settings in accordance with policy. Effective physical access control includes restricting authorized individuals to the server room and monitoring of access.

It was noted that the Agencies' processes for assigning and removing access are informal or undocumented for some systems. For other systems, formal procedures have been documented but it was noted that they were not followed consistently. Sample-based testing found examples where there was either no documented approval or inappropriate approval to support access that was granted to users, including

privileged users, and where accounts belonging to terminated employees were not removed in a timely manner. In addition, there is no requirement for regular review of user accounts and access privileges, which increases the risk of unauthorized access remaining undetected. Shared administrator accounts and the ability to access the administrative console from non-administrative workstations were also noted.

There is also no formal Council password standard. A password "standard" is contained in one procedural document; however, there is confusion as to whether this applies to all applications and infrastructure, as it is not defined within the document. As a result, password strength settings (minimum length, complexity, expiry, etc.) vary across applications and infrastructure. While some systems exceed minimum standards or have password settings configured in line with leading practices, several others were not in line with leading practices.

It was noted that some personnel, including a third-party company, have access to the server room without evidence of approval, and there is no documented process regarding removal of access rights to the server room. In addition, the server room and immediate surroundings are not monitored.

Recommendation: It is recommended that all user administration procedures, including those for physical access, be formalized, and existing procedures be communicated to staff to ensure they are followed consistently. User administration procedures should include requirements for the periodic review of all accounts and to document the use of administrator and privileged accounts. Furthermore, a password standard should be defined in line with leading practices, and existing passwords should be reviewed and brought into line with this standard. A procedure for the monitoring of physical access to the server room should be developed and implemented.

3.2.5 Vulnerability Management

Vulnerabilities should be managed through a process of continuous discovery and solution implementation. It was found that while security alerts are monitored and action is taken to deal with vulnerabilities, there is no record of actions taken in response to cyber alerts and it was not always possible to determine if the mitigation measures recommended by Lead Security Agencies[2] have been addressed. Some alerts or mitigation measure within alerts could easily be missed. Audit testing demonstrated a lack of follow-through on a critical security issue. While a risk management process is laid out in the Information Technology and Support Services (ITSS) Infrastructure Governance document, there are no specified requirements for documenting risk management decisions related to vulnerabilities.

The TBS Management of Information Technology Security states that vulnerability assessments (i.e., technical vulnerability testing) should be conducted "regularly on highly sensitive or highly exposed systems, and on a discretionary basis on other systems." While IT staff explained that technical vulnerability testing is undertaken on a periodic basis, no process or results of vulnerability testing were evident during the audit period.

It was noted that significant improvements have been made with regards to infrastructure patch management, including the implementation of an automated patch

[2] Lead Security Agencies are defined in the Policy on Government Security. They provide advice, guidance and services to support the day-to-day security operations of departments. Lead Security Agencies include agencies such as the Communications Security Establishment and Public Safety Canada.

management tool. That being said, certain network components are not currently patched and applications are not patched on a regular basis.

Recommendation: It is recommended that the vulnerability management process be reviewed and brought into line with leading practices, including the process for escalation and communication of vulnerabilities, and documenting risk management decisions. The technical vulnerability testing process should also be reviewed, formalized and applied on a regular basis. Evidence of vulnerability testing and follow-up on identified vulnerabilities should be retained for audit trail purposes. In addition, it is recommended that the patch management process be reviewed, formalized and extended to all network components and application systems.

4 Conclusion

There is a current focus on IT security and a number of improvements to the IT security program are currently underway at the Agencies. Nevertheless, it must be emphasized that the program requires critical governance elements, a complete policy and managerial framework and informal processes and procedures that are formalized and documented to reduce the risk of breaches to IT security.

5 APPENDIX A - Audit Criteria

Audit Criteria	
IT Security Program Governance	
1.1	A governance structure for IT security is established. Those charged with governance have clearly communicated mandates, are actively involved, have a significant level of influence, and exercise oversight of management processes. The oversight body meets regularly and reviews information related to IT security priorities and plans, provides advice on issues, reviews performance of the IT security function, and communicates its decisions to the organization in a timely manner.
1.2	A current IT Security Plan has been defined, and aligns business strategy, business expectations, and IT capabilities. The Strategic Plan is translated into tactical plans.
1.3	The organization's approach to managing IT security and its implementation are reviewed independently at planned intervals, or when significant changes to the security implementation are made.
IT Security Program Framework	
2.1	An IT Security Policy is defined and approved by management, published and communicated to all employees.
2.2	The IT Security Policy states management commitment and sets out the organization's approach to managing information security.
2.3	The IT Security Policy is supported by key procedures, standards and directives, and adheres to the Treasury Board of Canada Secretariat policy.
Boundary/Perimeter Defence	
3.1	Boundary/perimeter zones have been defined and are appropriately managed and controlled in order to be protected from threats and to maintain system and application security.
3.2	Internal IT security zones have been defined and are appropriately managed and controlled in order to be protected from threats and to maintain system and application security.
Access Controls and Privileged Access to Systems	
4.1	A formal authorization process is in place for assigning and removing user access to systems; user access rights to the NAMIS, AMIS, and SharePoint and related systems, and data are in line with defined and documented business needs, are requested by user management, and are approved by system owners.
4.2	Management performs regular reviews of all accounts and related privileges.
4.3	Password settings for applications and networks are managed in accordance with approved security policies.
4.4	Access to privileged application, database and network accounts is restricted and activities performed using these accounts are monitored.
Change and Configuration Management	
5.1	A process to manage configurations is established and appropriately maintained.
5.2	A process to manage system changes is established and maintained, and includes IT security input.
Vulnerability Management	
6.1	Vulnerabilities are managed through a process of continuous discovery and solution implementation.
6.2	Infrastructure runs a patch management system that permits prompt installation of critical security patches for NAMIS, AMIS, and SharePoint and related systems and databases and infrastructure.
Physical Security of Server Room	
7.1	Physical access restrictions are implemented and administered to ensure that only authorized

Audit Criteria	
	individuals have access to the server room. Management approval is required before access is granted.

6 Management Response to Audit Recommendations

Summary

NSERC and SSHRC management accept the findings of the audit.

Management agrees with the central theme of the audit that the significant improvements in IT security need to be leveraged and formalized to inform a culture of continuous improvement in order to deliver continued successful results and greater value to the Agencies' business.

The audit reveals areas for improvement within the IT security policy framework and proposes several ways in which these improvements may be acted on. This management response addresses each of the recommendations in turn and sets out comprehensive actions to ensure continued improvement for the Agencies' security posture.

While NSERC and SSHRC management recognize the overarching theme among the audit recommendations, it needs to be clearly noted that in the case of each of the recommendations, the issues had been previously identified, and specific actions were underway to rectify any shortcomings. As a result of the Independent Security Assessment in April 2011, an IT security policy framework was developed and used as a roadmap to address specific gaps. As well, during the timeframe of the audit, an IT security policy and directives were completed (November 2011), presented to a senior management table and formally approved by the Presidents (July 2012).

The security state of preparedness of the Agencies remains a critical priority for NSERC and SSHRC management.

Background

NSERC's and SSHRC's Corporate Internal Audit Division conducted an audit of the Agencies' joint IT security program. The audit examined the state of the IT security program and related activities between April 1, 2011 and the end of December 2011. The objectives of the internal audit assignment were to assess and report on the effectiveness of selected NSERC and SSHRC IT security controls.

Over the past 20 months, the security posture of the Agencies has been an area of critical focus for the Common Administrative Services Division (CASD) with specific emphasis on IT security. To that end, an independent IT security assessment was conducted in April 2011 and a departmental threat and risk assessment was completed in December 2011. These two initiatives identified the need for the continued formalization of IT security processes, a review of user access controls and the implementation of a vulnerability management program.

In July 2012, a bi-agency IT security policy was approved by the presidents, with overall responsibility for future directives and standards delegated to the VP of CASD. Responsibility for on-going maintenance, sponsorship and coordination of IT policies, including the IT Security Policy, rests with the Chief Information Officer (CIO).

Item	Recommendation	Action Plan	Target Date
1	A) Re-examine the IT security program governance structure and include senior management oversight of the program under the mandate of one of the existing senior committees/governance bodies to carry out the regular reviews of IT security priorities, plans and performance and to communicate the importance of the function to the organization.	• All IM and IT policies are reviewed and recommended for approval by the Agencies' Presidents to the IM/IT Bi-Council committee. • Information management is currently a standing item on the IM/IT Bi-Council committee agenda. • IT security will be added as a standing item for all future bi-agency committee meetings. • In conjunction with the DSO, a formal security communications strategy to inform and remind staff is being developed.	COMPLETE February 2012 Q4 2012-2013
	B) Develop a Departmental Security Plan as required by the Treasury Board Directive on Departmental Security Management, and include regular reviews of the IT security program.	• The development of a Departmental Security Plan (DSP) was initiated in March 2010 under the responsibilities of the Departmental Security Officer (DSO). • The DSP will include an annual review of the IT security program.	Q4 2012-2013
2	A) Finalize and approve the IT Security Policy and communicate to all employees.	• The agencies' IT Security Policy and corresponding directives were approved by the Agencies' Presidents in 2012.	COMPLETE July 2012

	B) Undertake a thorough review of its IT security framework, including the IT Security Policy, directives, standards, guidelines and the processes and procedures needed to implement them within the Agencies' operational context. This review should be conducted within the context of the latest Treasury Board and Lead Security Agency policy, directives, standards and guidelines and should ensure that security control objectives and controls as well as risk management are integrated into the Agencies' IT security program.	• The security policy framework, completed in November 2011, was used as the roadmap for the development of the current IT Security Policy and corresponding directives. • This framework has been developed in line with the IT security provisions of the Government of Canada's Policy on Government Security and the related Operational Security Standard: Management of Information Technology Security (MITS). • The MITS Standard defines baseline security requirements to which the Agencies must adhere in order to ensure the security of information and information technology assets under their control. • The framework also utilizes the organizational structure of standard ISO 27002, with each of the eleven categories referenced in the standard included as individual components.	Q4 2012-2013
3	A) Formalize the security and change management processes and develop procedural documentation to support operations to ensure that processes and procedures are followed consistently.	• A formal change control process is currently implemented within IIS with all proposed changes overseen by a Change Control Board (CCB) and a formal Request for Change process (RFCP). • Procedural documentation to support the security management process is under development for implementation.	COMPLETE August 2011 Q4 2012-2013
	B) Retain documentation of key controls (e.g. approvals, security reviews, change management documentation, etc.) for audit trail purposes.	• Procedural documentation and processes are being finalized for all security and change activities for audit purposes.	Q4 2012-2013

4	A) All user administration procedures, including those for physical access, be formalized, and existing procedures be communicated to staff to ensure they are followed consistently. User administration procedures should include a requirement for periodic review of all accounts, and to document the use of administrator and privileged accounts.	• Identified as a key requirement of the CRM and SharePoint implementations, all user administration procedures are being reviewed and formalized along with a threat risk assessment. • Two new monitoring tools have been implemented within the production environment to audit the use of privileged administrative accounts. Further a central password vault has been implemented to audit and track the use of all privileged system accounts and to monitor activities.	Jan 2013 COMPLETE April 2012
	B) A password standard should be defined in line with leading practices and existing passwords should be reviewed and brought into line with this standard. A procedure for monitoring of physical access to the server room should be developed and implemented.	• Identified as a key requirement of the CRM and SharePoint implementations, password standards have been established in line with industry best practices. • In conjunction with the DSO, procedures for the monitoring of physical access of the server room are being developed.	COMPLETE May 2012 Q4 2012-2013
5	A) Review the vulnerability management process and bring it into line with leading practices, including the process for escalation and communication of vulnerabilities and documenting risk management decisions.	• As part of the implementation of the IT Security Policy Framework, work has begun to formalize the vulnerability management process, including best practices from an audit and documentation perspective.	Q1 2013-2014
	B) Review, formalize and apply on a regular basis the technical vulnerability testing process. Evidence of vulnerability testing and follow-up on identified vulnerabilities should be retained for audit trail purposes.	• Implementation of new testing tools and procedures in support of vulnerability testing are scheduled to begin in Q4 for implementation in next fiscal year.	Q1 2013-2014
	C) Review and formalize the patch management process, and extended it to all network components and application systems.	• The patch management process has been formalized and automated through newly automated patching and monitoring tools.	COMPLETE March 2011

		• A new compliance officer position has been created to independently monitor and review patch and license compliance on the Agencies' infrastructure.	January 2012