Public Safety Canada | Sécurité publique Canada


# Public Safety Canada

# Internal Audit of Information Technology Security

April 30, 2020

Canada

Cat. No.: PS4-263/2020E-PDF
ISBN: 978-0-660-35034-9

## Table of contents

## Executive Summary

The objective of this audit was to assess the adequacy and effectiveness of the management control framework over information technology (IT) security[1] at PS, as well as its readiness to comply with the newly revised Treasury Board (TB) *Policy on Government Security* and other relevant policies, directives and standards.

## Why this is important

Government of Canada departments are heavily reliant on various IT systems and processes to deliver their mandate. Securing these IT systems from cyber and other threats is essential to maintaining the confidentiality, integrity, and availability of the information within the systems.

To provide direction to manage government security in support of the trusted delivery of Government of Canada programs and services, a comprehensive update to the TB policy suite on security was approved in Spring 2019. The objective of the policy update was to better reflect the evolving dynamic operating environment and the need to ensure strategic leadership for government security in an enterprise IT and service delivery context. Overall, the changes were made to strengthen security management practices within departments, with partners and government-wide, and ensure an appropriate degree of preparedness in a dynamic risk environment.

## Key Findings

The audit found that:

- Public Safety has a governance framework in place to support the management of IT security activities; however, opportunities for improvements exist to ensure sound risk management practices and a more integrated approach to security management.
- The department has controls in place to manage key IT security activities; however, processes are not systematically followed and adequately monitored to ensure continued compliance and proactive risk mitigation.
- The department has established elements of an IT security training and awareness program; improvements are required to further ensure that employees understand their responsibility in protecting the confidentiality, availability and integrity of information.

[1] **IT security control framework**: All of an organization's resources, including policies, staff, processes, practices, controls, and technologies, to assess and mitigate IT security risks and attacks.

## Recommendations

### Recommendation 1:

The Assistant Deputy Minister (ADM), Corporate Management Branch (CMB) should review the existing governance framework to ensure alignment with the requirements of the new Treasury Board *Policy on Government Security* and improve strategic decision-making related to IT security, specifically:

- Ensure the consistent integration of IT security in the departmental security risk management process;
- Clarify roles and responsibilities of individuals and governance bodies for managing IT security activities; and,
- Ensure that the internal policy instruments, including policies, procedures and guidelines are updated, approved, communicated and reviewed regularly for continued relevance.

### Recommendation 2:

The ADM, CMB should, following a risk-based approach, ensure ongoing reviews and monitoring of the following key IT security activities for compliance with established processes for safeguarding sensitive departmental information:

- Management of IT systems access;
- Process to identify, assess and report IT security incidents;
- Prevention and management of loss, damage or compromise to the organization's information; and,
- Security considerations in Systems Development Life Cycle.

### Recommendation 3:

The ADM, CMB should ensure that an IT security awareness and training program is developed and implemented to comprehensively address risks related to IT security and ensure employees maintain the required knowledge to meet their responsibilities.

## Conclusion

Improvements are required for Public Safety Canada to establish a well-defined and fully effective control framework over IT security activities that complies with the newly revised TB *Policy on Government Security*, and other relevant policies, directives and standards. More specifically, significant efforts are required by PS to document, communicate and ensure compliance with IT security control practices required by Treasury Board.

# 1 Introduction

## 1.1 Background

Government of Canada departments are heavily reliant on various Information Technology (IT) systems and processes to deliver their mandate. Securing these IT systems from cyber and other threats is essential to maintaining the confidentiality, integrity, and availability of the information within the systems.

Shared Services Canada (SSC) is responsible for securing the underlying IT infrastructure on which over 40 government organizations' IT systems operate. Departments, including Public Safety Canada (PS) are responsible for implementing security controls to meet departmental IT security requirements, in accordance with departmental practices. While SSC must manage and secure PS' infrastructure, PS must manage and secure its own applications, data, and desktop devices used to maintain the integrity of information within its IT systems.

To provide direction for the management of government security in support of the trusted delivery of programs and services, a comprehensive update to the Treasury Board (TB) policy suite on security was approved in Spring 2019. The TB *Policy on Government Security* and related directives and standards came into effect July 2019, while the TB *Policy on Service and Digital* will come into effect in April 2020. These replace the TB *Policy on Government Security* of 2009, the TBS *Directive on Departmental Security Management* of 2009 as well as numerous TB Operational Security Standards, such as the Management of Information Technology Security (MITS).

The objective of the policy update was to better reflect the evolving operating environment and the need to ensure strategic leadership for government security in an enterprise IT and service delivery context. Overall, the changes were made to strengthen security management practices within departments, with partners and government-wide, and ensure an appropriate degree of preparedness in a dynamic risk environment.

The policies and related directives have been updated namely to:

- Streamline instruments and rules;
- Strengthen governance, through the mandatory appointment of a Chief Security Officer (CSO);

- Clarify roles and responsibilities for the lead security agencies (which includes Public Safety Canada) and internal enterprise service organizations[2] (e.g. Shared Services Canada); and,
- Strengthen community and culture through the establishment of new training and new security guidance and tools to standardize and modernize business practices.

The appointment of a CSO replaces the former policy requirement for the designation of a Departmental Security Officer (DSO), as a means to render a more strategic role to the function. The CSO's role includes providing leadership, coordination and oversight for departmental security activities and complements the existing operational expertise and leadership in the department. CSOs are expected to work with partners to ensure security is managed effectively. The Deputy Minister of PS appointed the Assistant Deputy Minister (ADM) of the Corporate Management Branch and Chief Financial Officer (CFO) as the new CSO, effective October 17, 2019.

Under the revised policy, deputy heads are also responsible for designating "senior officials" who have responsibility for the security aspects of a program, service or activity area or for a security function. Senior officials may include program officials, chief financial officers, chief audit executives, chief information officers, chief privacy officers and other officials designated pursuant to a statutory requirement. PS is in the process of reviewing its governance structure to support the new CSO function and the requirement of the TB policy, including the designation of senior officials and their corresponding roles and responsibilities.

## 1.2 Audit Objective and Scope

The objective of this audit was to assess the adequacy and effectiveness of the management control framework over IT Security[3] at PS, as well as its readiness to comply with the newly revised TB *Policy on Government Security* and other relevant policies, directives and standards.

The scope of this audit included activities related to departmental IT security for the period of April 1, 2018 to September 30, 2019, but also included a review of other pertinent documents outside of these dates. The audit focused on the IT security activities under the responsibility of PS and related to the corporate network.

[2] As per the 2019 *Policy on Government Security*, an internal enterprise service organization is "a department or organization that provides internal enterprise services to other Government of Canada departments. This includes lead security agencies that deliver government-wide security services".
[3] IT security control framework: All of an organization's resources, including policies, staff, processes, practices, controls, and technologies, to assess and mitigate IT security risks and attacks.

The scope of the audit did not include:

- Communication Security equipment (cryptographic items), the Government of Canada Secret Infrastructure (GCSI) and the Canadian Top Secret Network (CTSN), as they are subject to periodic external audit/review.
- IT infrastructure and services provided by SSC or other third party service providers. Some communications between PS and other departments has been reviewed, but a direct review was excluded.

### 1.3 Methodology and Audit Approach

For each criterion established, an audit methodology was developed to adequately examine the area to support the objective. Methodology or approach refers to the work involved in gathering and analyzing information to achieve audit objectives. This work ensures that sufficient and appropriate audit evidence was collected to enable the audit team to draw conclusions related to each audit objective.

To complete the audit, the following methods were used:

- Interviews with personnel with respect to the management of IT security and related activities;
- Review of applicable TB and departmental policy instruments and procedures for the management and administration of the IT security function;
- Review of supporting documentation, including committee meeting records of decisions; and,
- Process walkthroughs, testing and analytical review.

### 1.4 Conformance with Professional Standards

This audit conforms to the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing and the Government of Canada's *Policy on Internal Audit*, as supported by the results of the Quality Assurance and Improvement Program.

## 2 Findings and Recommendations

### 2.1 Finding 1: Public Safety has a governance framework in place to support the management of IT security activities; however, opportunities for improvements exist to ensure sound risk management practices and a more integrated approach to security management.

Within a department, adequate processes and structures should be in place to ensure that senior management possesses sufficient and reliable information to inform, direct, manage and monitor the organization's IT security activities. The governance and oversight mechanisms should foster risk-based decision-making, while considering all security controls through an integrated management approach.

**Governance and risk management process**

During the course of the audit, the DSO, Chief Information Officer (CIO), Director of IT Security/Information Security Officer, and the IT Security Coordinator (ITSC) worked collaboratively to ensure that appropriate security measures were applied to all departmental assets, activities and processes.

The corporate security program within PS was led by the DSO, an executive in the Corporate Services Directorate. The DSO was responsible for ensuring the coordination of all security policy functions and the implementation of security policy requirements.

The management of the department's information and IT assets, including operational responsibility for IT security, was under the responsibility of the CIO Directorate (CIOD).

The Directorate is separated into three divisions:

- Client Services and Applications;
- Information Management (IM); and,
- IM/IT Security, Portfolio Management and interoperability.

The ITSC (in the IM/IT Security and Portfolio Management Division) was responsible for the overall management and coordination of the Departmental IT Security Program, the IT Security Directive and related issues.

Although PS did not have a governance body dedicated to IM and IT matters, the Departmental Management Committee (DMC) and Resource Management Committee (RMC) were the two main senior-level governance bodies supporting departmental IM and IT activities, including security-related issues. During the scope of the audit, discussions on IM and IT Security at DMC and RMC meetings included an overview of the annual IT Plan 2019-2020 and a presentation of the quarterly IT and IM dashboard, which presents general data on IT and IM issues. The CIO also informed the audit team that he holds periodic meetings with executives of the various branches to discuss IM and other IT matters as necessary (e.g. the recent migration to the Windows 10 operating system).

Given the increased importance of the subject, interviewees indicated that there is insufficient time allocated during DMC and RMC meetings to discuss and set strategic direction on IT security matters, such as IT security incidents, IT architecture, and IT policies and directives.

Pursuant to the 2019 TB *Policy on Government Security*, the Deputy Head is responsible for approving a three-year departmental security plan (DSP); this plan is also reviewed annually. The DSP is an essential tool for deputy heads to set direction and priorities for security management. It should provide a comprehensive view of all security control areas and related risks in order to outline strategies, goals, objectives, priorities and timelines for improving departmental security. During the course of the audit, the DSO led the development of the DSP.

The PS DSP for 2017-2020 did not include IM and IT security matters. These were intended to be covered in the Departmental IM-IT Plan for 2019-2022, which is developed by the CIO.

While there was awareness within the CIOD that there are IT security risks within the department, there is currently no formal mechanism used within PS to systematically identify, analyze and evaluate these risks (such as through the use of a risk register or other similar tool). IT security activities, such as responding to IT security incidents, are conducted daily to support PS' mandate, however, they are conducted on a best effort basis depending on availability of resources and are not formally documented, rather than planned from the results of a comprehensive risk management process.

IT security risks are known to the department on an informal basis; however, opportunities to improve processes for the management of these risks exist in order to ensure that all significant risks are identified, recorded, investigated, resolved and reported in a timely manner for appropriate oversight and decision-making. Failure to effectively and formally identify and manage IT security risks could result in resources not being attributed in accordance with management priorities and risk tolerance.

Improvements to departmental risk management practices for IT security and oversight mechanisms were occurring during the course of the audit: PS had started drafting a security risk register and CIOD conducted a Security Control Assessment to outline an inventory of IT security controls, identify control gaps and draft recommendations to address the gaps. Both are intended to inform the first year of the 2020-2023 iteration of the DSP and ensure a more integrated approach to security management. Further, the governance structure was under revision to support the role of the newly appointed CSO.

To align with the new governance-related requirements in the TB policy suite, further revision and clarification of senior officials' roles, responsibilities, and accountabilities should be considered, in both internal guidance documentation and job descriptions.

### Policies, procedures and guidelines

There are currently three policies, one directive, approximately 30 standards, and one guide related to security at PS, most of which were last updated in 2011. Many of these

PS policy instruments refer to governance bodies, positions or terminology that are obsolete. For example, the PS *Directive on IT Security* refers to the Departmental Security Committee which no longer exists, and to the Certification and Accreditations process which has been superseded by the security assessment and authorization process. The policy instruments also do not include references to the delineation of roles between PS and SSC for securing IT infrastructure, given that the latter was created after the update of the majority of the policy instruments in place.

While management is cognizant of the requirement to update the departmental security policy instruments to align them with the new TB policy suite, work on the update had not yet started during the course of the audit. Additionally, the process for approving policy instruments is not well defined at PS. The majority of the policy instruments were approved by the CIO, some by the DMC, and for a few, confirmation of approval could not be found.

To ensure compliance with organizational security policies and standards, policy instruments must be communicated to all employees. The audit found that existing policy instruments are not readily available to employees. While some departmental policy instruments are available in PS's information management system or on the departmental intranet, the audit team was unable to ascertain that the guidance and policy instruments accessed were the latest approved versions in some cases. The audit did not find a robust communication strategy in place to inform stakeholders of policy instruments as well as their responsibilities for IT security. Clear and formalized communication of roles and responsibilities contribute to a culture of accountability and help ensure compliance.

**Recommendation 1:**

The Assistant Deputy Minister (ADM), Corporate Management Branch (CMB) should review the existing governance framework to ensure alignment with the requirements of the new Treasury Board *Policy on Government Security* and improve strategic decision-making related to IT security, specifically:

- Ensure the consistent integration of IT security in the departmental security risk management process;
- Clarify roles and responsibilities of individuals and governance bodies for managing IT security activities; and,
- Ensure that internal policy instruments, including policies, procedures and guidelines are updated, approved, communicated and reviewed regularly for continued relevance.

## 2.2 Finding 2: Public Safety has controls in place to manage key IT security activities; however, processes are not systematically followed and adequately monitored to ensure continued compliance and proactive risk mitigation.

Sufficient and adequate operational controls should be in place to mitigate key IT security risks and should work as intended. More specifically, the audit looked at whether:

- Access controls to IT systems are implemented and reviewed periodically to protect IT systems and prevent unauthorized access to information;
- An effective process to identify, monitor, analyze, assess and report IT security incidents in a timely manner is in place;
- Adequate controls are in place to prevent loss, damage, or theft of the organization's electronic information; and,
- Adequate controls are in place in the IT system development process to prevent IT systems from being implemented or changed without adequate security safeguards.

### Access Controls to IT Systems

The audit focused on the management of administrative privileges access controls as it is one of the top 10 IT security actions to protect internet-connected networks identified by the Communications Security Establishment Canada (CSEC). The 2019 TBS *Directive on Security Management* requires that departments establish measures to define access privileges based on departmental security requirements, segregation of duties, and acceptable use of government information system to control the use of accounts that have administrative privileges. This includes restricting the number of users who have such privileges. In principle, the least amount of privileged access should be granted and access should be based on an as-required basis. The *Directive* also requires departments to review access privileges periodically, and remove access when it is no longer required (for example, when an employee changes responsibilities or leaves the department).

SSC is responsible for maintaining access controls, including privilege accounts for all infrastructure accounts including network and email access, whereas PS is responsible for informing SSC of the valid accounts. In accordance with the 2011 PS Standard on IT Systems Access, the ITSC is responsible for monitoring compliance with the standard on system access. However, account management is mainly exercised by the Client Services and Applications Division and, in some circumstances, the business owners (i.e. end users) of the system may retain some account management responsibilities (e.g. RDIMS and SAP).

The audit found that there is no documented process for the regular monitoring of access management. Access control review is performed on an ad hoc basis by the Client Services and Applications Division based on the availability of resources. The IM/IT Security Division does not conduct periodic reviews or ongoing monitoring of access privileges.

In addition, departed employees still had privileged access to the network and some current employees had unnecessary administrative access to mission critical applications. Removal of access privileges for indeterminate employees is reliant on a departure form being submitted by the employee; however, we were advised that departure forms are sometimes omitted when an employee leaves the department or changes responsibilities within the organization.

During the course of the audit, PS implemented a new monitoring software tool to help manage access to privileged accounts. The privileged account access monitoring tool allows the IM/IT Security Division to monitor the use of elevated and administrative rights on all PS devices, as well as providing a means to replace the need for these elevated rights locally by empowering the tool to perform chosen tasks on the users behalf. However, there was insufficient evidence to suggest that a periodic review of the users with administrative privileges was conducted to supplement this tool and to verify that accounts were being managed effectively.

### IT Security Incident Management

The TB *Policy on Government Security* defines a security event as any event, act, omission or situation that may be detrimental to government security, including threats, vulnerabilities and security incidents. A security incident, on the other hand, is defined as any event (or collection of events), act, omission or situation that has resulted in a compromise. Incidents can be deliberate or accidental.

Practices for security event management must be defined, documented, implemented and maintained to monitor, respond to and report on threats, vulnerabilities, security incidents and other security events, and ensure that such activities are effectively coordinated within the department, with partners and government-wide, to manage potential impacts, support decision-making and enable the application of corrective actions. IT security events and incidents may be identified from various sources such as the antivirus/anti-malware tools, weekly reports from the Canadian Cyber Security Centre, security sweeps, emails from the National Institute of Standard and Technology, notifications through the PS security mailbox or helpdesk, or reported directly to the DSO or the CIO.

There is no formal tracking of IT security incidents at PS. Pursuant to the PS Standard on IT Security Incident Management, IT staff must ensure there are mechanisms in

place to enable the types, volumes and costs of IT security incidents to be quantified and monitored, and it is the responsibility of the ITSC to oversee the IT security incident handling activities. IT security staff indicated that IT security incidents are addressed as they are received or detected. The audit team was informed that only 4 or 5 IT security incidents have been reported and/or investigated in the last two years; however, we could not confirm this because there are no documented files or report.

Significant improvements to the IT security incident management process at PS are required. The audit could not confirm that all IT security incidents were recorded and acted upon through the appropriate channels to ensure that timely corrective actions were taken. This would allow PS to have a more accurate picture of the number and types of IT security incidents to establish the overall departmental threat level and react accordingly.

### Security of Information Management Assets

The TB *Policy on Government Security* requires that "IM security requirements, practices and controls [be] defined, documented, implemented, assessed, monitored and maintained throughout all stages of the information life cycle to provide reasonable assurance that information is adequately protected in a manner that respects legal and other obligations and balances the risk of injury and threats with the cost of applying safeguards".

PS creates, stores and transmits information on three government networks:

- the PS corporate network (RDIMS) supported by SSC, for Protected information up to Protected B security level;
- the GCSI network supported by SSC, for classified information up to Secret security level; and,
- the CTSN supported by CSEC, for classified information up to Top Secret security level.

Electronic records generated by PS are in large part stored in RDIMS. While the scope of the audit did not include a review of the information stored in the GCSI and the CTSN, the audit considered the controls in place to prevent Secret and Top Secret information from being stored on the corporate network (RDIMS).

DMC receives quarterly dashboards on IT and security updates that are used for monitoring purposes. The dashboard for Q1 2019-2020 prepared by CIOD and presented at RMC indicated that approximately [Redacted] above the acceptable Protected B level were stored in RDIMS. This issue could be due to a number of factors, including over classifying of documents by PS employees, lack of enforcement, limited awareness of electronic document handling standards, and/or difficulty using and

accessing the GCSI. The audit team did not attempt to determine if the documents had been over classified. During the course of the audit, this number was reduced to [Redacted], and the ability for users to select a classification level above Protected B when saving a document in RDIMS was removed. In addition, CIOD staff were working with individual branches to advise them on the review and application of document classification levels and, when necessary, to migrate the documents from the corporate network to the appropriate network.

There are very limited activities to monitor compliance with information security requirements at PS. For example, approximately [Redacted] as either Protected or Classified were available to all users in RDIMS during the course of the audit; however, not all users would necessarily possess the required security clearance to access these documents. There is no periodic review or testing of the documents stored in RDIMS to determine if they have been adequately classified.

There is limited awareness of electronic document handling requirements and the use of secure electronic transmission tools (e.g. Entrust) by PS employees. Transmitting sensitive PS information or documents to personal email addresses without additional protection such as encryption is also not monitored. Without adequate practices and controls to ensure that information at PS receives an appropriate level of protection, there is a risk that information may not be classified appropriately or handled in terms of its sensitivity and criticality to the organization.

The TBS *Information Technology Policy* Implementation Notice for the *Secure use of portable data storage devices within the Government of Canada* requires that all departments maintain records of the portable data storage devices issued within their organization. All portable storage devices must be password or biometric controlled and the information stored on them encrypted. This supplements but does not replace physical security procedures. The audit found that PS does not maintain records of USB keys that have been issued and that there are limited controls in place to identify if individuals are saving sensitive information on a USB key. In addition, PS does not pick up USB keys during physical security sweeps to examine their content. There is thus a risk that USB keys contain unencrypted sensitive information that could constitute a security incident.

Data on all PS laptops should be encrypted using a cryptographic module approved by CSEC. The audit team reviewed standard imaging for laptops and tablets that have been migrated to the Windows 10 operating system and noted that they are encrypted using [Redacted], which is a cryptographic module approved by CSEC. Moving forward, the department intends to encrypt all data stored on desktops and laptops and disable all USB ports by default when the upgrade to Windows 10 is fully implemented throughout the department.

Without an adequate process to control portable data storage devices, there is a risk that sensitive information may not be adequately protected against unauthorized access and disclosure.

### Security Controls for IT systems and applications

The TBS *Directive on Security Management* requires that all IT systems be assessed and authorized prior to operation by completing the security assessment and authorization (SA&A) process. Similar to the former Certification and Accreditation process, the purpose of the SA&A process is to verify that the security requirements established for a particular system or service are met and that the controls and safeguards work as intended before a system is put in production.

PS developed a Security Assessment & Authorization Guide in 2016 for the SA&A process, as well as a Standard on Change, Configuration and Release Management, a Standard on IT Security in the Systems Development Life Cycle (SDLC), and a Change Control Board. The IM/IT Security Division is responsible to manage the SA&A process, which indicates that a number of IT security requirements must be completed before a system is allowed to be in production:

- System Profile Description;
- Statement of Sensitivity (SoS);
- Concept of Operations;
- Security Requirements Traceability Matrix (SRTM);
- Privacy Impact Assessment (if the system contains personally identifiable information); and,
- Vulnerability Assessment.

After completion of the SA&A process, the IM/IT Security Division prepares the SA&A report recommending operational approval. An IT system can receive a full authority to operate, an interim authority to operate or no authority to operate.

While there are approximately 50 IT systems and applications at PS, the audit focused on the six applications identified by the department as mission critical. The audit found that all six mission critical applications do not have the required SA&A report in place, which means that the applications are in production without a valid Authority to Operate (AO) and could be at risk of containing unknown security vulnerabilities. PS has recognized this issue and included it in its draft security risk register.

PS has established a Change Control Board that is responsible for all proposed configuration management or system changes. Prior to implementation of system changes, the IT Security SA&A Report as well as the Authority to Operate must be updated by the IM/IT Security Division.

The audit team tested two recent major changes to mission critical applications to determine if the IT security impact of the changes were assessed and if they complied with the change management process. The two selected changes were:

1. Newsdesk: Twitter integration (December 2018).
2. RDIMS: Upgrade to RDIMS (July 2019)

The audit found that the Newsdesk system change was implemented without informing or notifying the IM/IT Security Division as such, the potential impact of the Newsdesk system change was not assessed.

For the upgrade to the RDIMS system, a representative from IT security was present during the discussion at the Change Control Board, but neither a documented analysis of IT security impacts nor an Authority to Operate were noted.

Non-compliance with the established process could allow for the possibility that the changes to IT systems and applications were implemented without full consideration of the IT security impacts and could result in security vulnerabilities being introduced to existing IT systems and applications.

**Recommendation 2:**

The ADM, CMB should, following a risk-based approach, ensure ongoing reviews and monitoring of the following key IT security activities for compliance with established processes for safeguarding sensitive departmental information:

- Management of IT systems access;
- Process to identify, assess and report IT security incidents;
- Prevention and management of loss, damage or compromise to the organization's information; and,
- Security considerations in Systems Development Life Cycle.

## 2.3 Finding 3: Public safety has established elements of an IT security training and awareness program; however, improvements are required to further ensure that employees understand their responsibility in protecting the confidentiality, availability and integrity of information.

The security of information technology and the information it contains is the responsibility of all employees, not just that of the IM/IT Security Division. The new TB *Policy on Government Security* and the TBS *Directive on Security Management* requires that each department define, document and maintain departmental security awareness and training requirements and practices, in accordance with government-wide policy requirements. Departments must develop, deliver, document and maintain security awareness activities and products to inform and remind individuals of security

threats and risks and of their security responsibilities. Departments must also provide or arrange security training to all employees, including specialized security training for those individuals who have specific security responsibilities such as the COMSEC custodian.

In 2019-20, the DSO developed a Security Awareness Strategy which requires all employees to complete two security-related courses upon their arrival in the department. The first mandatory course is titled Security Awareness (A230) and is offered by the Canada School of Public Service. The audit team obtained confirmation that the compliance rate for PS employees with this mandatory course was 87% as of August 2019. The second course is a mandatory 20-minute security briefing video that all staff (employees and contractors) must complete during onboarding in order to receive their building access pass.

While not specifically focused on IT security, both mandatory courses cover basic elements of IT security and are well presented. PS has not established a training and awareness program specific to IT security, nor has it established a requirement for refresher training on security awareness at periodic intervals to bring staff up-to-date of new threats and trends in IT security.

PS does not conduct practical exercises in security awareness amongst its employees to increase awareness on how to respond to suspected security incidents (e.g. phishing exercises). The security sweep procedure does not incorporate the assessment of key security controls, such as unattended and unprotected USB devices or laptop computers left physically unlocked. The sweeps do record if computers are left logged in and unlocked by the user.

Security awareness and training should be conducted systematically and comprehensively to ensure that individuals are informed of their IT security responsibilities and maintain the necessary knowledge and skills to effectively carry out their functions. This would contribute to providing reasonable assurance that PS employees will not knowingly compromise security and that they understand the potential consequences of not meeting their security responsibilities.

**Recommendation 3:**

The ADM, CMB should ensure that an IT security awareness and training program is developed and implemented to comprehensively address risks related to IT security and ensure employees maintain the required knowledge to meet their responsibilities.

# 3 Conclusion

Improvements are required for Public Safety Canada to establish a well-defined and fully effective control framework over IT security activities that complies with the newly revised TB *Policy on Government Security*, and other relevant policies, directives and standards. More specifically, significant efforts are required by PS to document, communicate and ensure compliance with IT security control practices required by Treasury Board.

# 4 Management action plan

| Recommendation | Actions Planned | Target Completion Date |
|---|---|---|
| 1. The Assistant Deputy Minister, Corporate Management Branch should review the existing governance framework to ensure alignment with the requirements of the new Treasury Board *Policy on Government Security* and improve strategic decision-making related to IT security, specifically:<br>• Ensure the consistent integration of IT security in the departmental security risk management process;<br>• Clarify roles and responsibilities of individuals and governance bodies for managing IT security activities; and,<br>• Ensure that the internal policy instruments, including policies, procedures and guidelines are updated, approved, communicated and reviewed regularly for continued relevance. | Define roles and designate a departmental Cyber Security Officer (CYSO) and Deputy Cyber Security Officer (D/CYSO), as part of a broader clarification of IT security roles and responsibilities internal to CIOD and CMB.<br><br>Define and distinguish respective IT security roles and responsibilities with our enterprise service providers: Shared Services Canada (SSC), Communications Security Establishment Canada (CSEC), Public Services and Procurement Canada (PSPC).<br><br>Create and maintain an IT Security Risk Registry based on the Departmental Security Plan (DSP) and Departmental risks.<br><br>Review ITSG-33 corporate security controls.<br><br>Full review of Public Safety Canada IT Security policies, procedures and guidelines.<br><br>Review and align Security Assessment & Authorization (SA&A) and Authority to Operate (ATO) processes. | 03/31/2021<br><br>03/31/2022<br><br>03/31/2021<br><br>03/31/2023<br><br>03/31/2023<br><br>03/31/2021 |

| | | |
|---|---|---|
| 2. The Assistant Deputy Minister, Corporate Management Branch should, following a risk-based approach, ensure ongoing reviews and monitoring of the following key IT security activities for compliance with established processes for safeguarding sensitive departmental information:<br>• Management of IT systems access;<br>• Process to identify, assess and report IT security incidents;<br>• Prevention and management of loss, damage or compromise to the organization's information; and,<br>• Security considerations in Systems Development Life Cycle. | Develop an investment plan laying out planned purchases of new IT Security tools in a staggered fashion as priorities and resources dictate.<br><br>Create and maintain a separate infrastructure for IT Security employees, devices and tools.<br><br>Have the Strategic Uptake and Project Review Board (SUPRB) enforce the consideration of IT Security throughout the lifecycle of all IM/IT tracked activities and projects.<br><br>Tracking log of security events, incidents and compromises.<br><br>Update or perform SA&A and ATO on all PS existing major and critical applications, prioritizing the critical.<br><br>Conduct regular administrative rights reviews and an audit of elevated privileged user activities on all systems.<br><br>Create and maintain an integrated calendar of all IT security activities, to facilitate planning and ongoing monitoring, reviews and analysis and ensure compliance with established policies and processes. | 03/31/2023<br><br>03/31/2021<br><br>03/31/2021<br><br>03/31/2021<br><br>03/31/2023<br><br>03/31/2021<br><br>03/31/2021 |

| | | |
|---|---|---|
| 3. The Assistant Deputy Minister, Corporate Management Branch should ensure that an IT security awareness and training program is developed and implemented to comprehensively address risks related to IT security and ensure employees maintain the required knowledge to meet their responsibilities. | Develop a communications and security awareness strategy.<br><br>Implement an inspection process for digital content.<br><br>Institute a special monitoring of high risks activities by users.<br><br>Implement periodic phishing and security testing programs. | 03/31/2021<br><br>03/31/2021<br><br>03/31/2021<br><br>03/31/2021 |

## Acknowledgements

The Internal Audit and Evaluation Directorate would like to thank all those who provided advice and assistance during the audit.

## Annex A: Audit Criteria

The following criteria were used to ensure sufficient and appropriate testing to support the audit objective and opinion:

| | |
|---|---|
| **Criterion 1** | An effective governance structure is in place to support planning, decision-making and monitoring related to IT security. |
| **Criterion 2** | Adequate and sufficient operational controls are in place to mitigate IT security risks and are working as intended. |

## Annex B: Acronyms

| | |
|---|---|
| CIO | Chief Information Officer |
| CMB | Corporate Management Branch |
| CSEC | Communications Security Establishment Canada |
| COMSEC | Communications Security |
| CSO | Chief Security Officer |
| DMC | Departmental Management Committee |
| DSO | Departmental Security Officer |
| DSP | Departmental Security Plan |
| GCSI | Government of Canada Secret Infrastructure |
| CTSN | Canadian Top Secret Network |
| IM | Information Management |
| IT | Information Technology |
| ITGC | Information Technology General Controls |
| ITPIN | IT Policy Implementation Notice |
| ITSC | Information Technology Security Coordinator |
| MITS | TB Operational Standard – Management of IT Security |
| NIST | National Institute of Standard and Technology |
| PKI | Public Key Infrastructure |
| PIA | Privacy Impact Assessment |
| PS | Public Safety Canada |
| RMC | Resource Management Committee |
| SA&A | Security Assessment & Authorization |
| SOS | Statement Of Sensitivity |
| SRTM | Security Requirements Traceability Matrix |
| SSC | Shared Services Canada |
| TB | Treasury Board of Canada |