Audit of Information Technology Security

Table of Contents

Acknowledgements

The audit team would like to thank those individuals who contributed to this project and, particularly, employees who provided insights and comments as part of this audit.

1.0 Executive Summary

1.1 Background

Information Technology (IT) is a Strategic Asset and Critical Enabler of the Government of Canada's commitment to deliver integrated and easily accessible services to Canadians, while ensuring that internal administrative operations are managed efficiently and effectively. The Treasury Board (TB) *Policy on Government Security* defines IT Security as the "safeguards" to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information.

In 2005, the Treasury Board Secretariat (TBS) requested that all departments implement by December 2006 the *Management of Information Technology Security Standard* (MITS). This standard represents the baseline IT security standards for all Government of Canada departments to follow.

In 2011-12 the IT environment across the federal government went through significant changes in the delivery of IT services. Shared Services Canada (SSC) was created as the vehicle for network, server infrastructure, telecommunications and audio/video conferencing services for the forty-three departments and agencies with the largest IT spend in the Government of Canada. Formal Business Arrangement agreements were put in place with each department, and underline the fact that departmental service levels would continue to be met.

Roles and Responsibilities

As per the TB *Policy on Government Security* issued under section 7 of the *Financial Administration Act* (FAA), Deputy heads are accountable for the effective implementation and governance of security and identity management within their departments and share responsibility for the security of government as a whole.

MITS describes roles and responsibilities for key positions, including the department's Chief Information Officer (CIO) who is responsible for ensuring the effective and efficient management of the department's information and IT assets.

Currently, roles and responsibilities for IT security are delineated between SSC and the CIOD and DSO, both of which are within the Corporate Management Branch.

1.2 Why it's Important

During the audit planning cycle, the department identified the risk of non-compliance with certain IT security aspects and requirements of the TB *Policy on the Management of Information Technology* and the *Policy on Government Security*. Further, given that no similar audits have been performed in the past at PS, there was a need to ensure that internal controls over the management of IT security at PS are adequate and effective.

We also note that 2012-13 will be the first year of operation for SSC having direct responsibility for the back-end IT security services, while CIOD retains overall responsibility for the stewardship of all IT Security resources and the efficient and effective delivery of IT security services. While there is a formal Business Arrangement agreement between PS and SSC, which underlines the fact that departmental service levels would continue to be met, it is not clear what the original PS service levels were.

1.3 Audit Objective and Scope

The objective of the audit was to assess the department's compliance with the TB *Policy on the Management of Information Technology* and the *Policy on Government Security*, focusing on IT security aspects and requirements. This included assurance that internal controls over the management of IT security were adequate and effective.

The audit period covered the timeframe from January 1, 2012 to June 30, 2012.

The scope of the audit included the following key areas:

- IT Security Planning
- IT Security Strategy and Governance
- IT Security Monitoring
- IT Security Risk Management
- IT Security Roles and Training
- System Configuration

- IT Security Management
- Incident and problem management

1.4 Audit Opinion

In my opinion, there are adequate and effective mechanisms in place to ensure the appropriate management of IT security, although some important areas require management attention to address some residual risk exposure.

1.5 Statement of Assurance

In the professional judgment of the Chief Audit Executive, sufficient and appropriate audit procedures have been conducted and evidence gathered to provide senior management with reasonable assurance of the accuracy of the opinion provided and contained in this report. The opinion is based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria. The opinion is applicable only to the entity examined.

1.6 Summary of Audit Findings

Throughout the audit fieldwork, the audit team observed many examples of how controls are properly designed and applied effectively. This resulted in several observed strengths across the audit areas.

The auditors found that a set of IT security policies, directives and standards were in place, and align with government and industry frameworks, policies and best practices. As well, various documents identifying priorities and projects for IT security exist. Additionally, the Departmental Security Plan identifies a formal governance structure which is integrated into the corporate governance structure.

The threat and risk assessment process, which is used to identify IT security risks for specific systems or applications, was found to be appropriately informed and used robust tools resulting in formal subject specific reports. The Protected B network was certified and a partial list of controls was identified.

User identification and access rights are managed through the Active Directory system within the Microsoft Windows operating system. The auditing tools part of the Active Directory and other similar tools are able to track IT activity performed by various network users.

Measures are in place to verify that all network devices are at current release and security patch levels. Additionally, security barriers are strategically placed at the network's perimeter, between the department's trusted internal network and non-trusted public (i.e., Internet), vendor (i.e., service organization) or business partner (i.e. extranet) segments thereby protecting the organization from external threats. Automated tools have been implemented to provide protection against viruses and to ensure that violations are appropriately communicated. The virus protection tool has been installed on workstations and includes virus definition files that are

centrally updated on a regular basis. Security tools are used to routinely monitor the network for security events.

Systems are configured to enforce user authentication before access is granted. Further, the requirements for passwords are defined in the Network Password Standard and Procedures and enforced accordingly.

The audit found elements of Configuration Management in place. A configuration policy exists requiring configuration items and their attributes to be identified and maintained, and that change, configuration, and release management are integrated. In addition, there is a Change Configuration Board that discusses and approves change configuration requests. The board meetings take place on a regular basis and only authorized personnel have designated access to the change configuration items.

The audit found that roles and responsibilities, specific to the department, are established, communicated, and understood. Additionally, the Chief Information Officer Directorate communicates to stakeholders and users throughout the department on an adhoc basis about relevant IT Security activities. Finally, Performance Agreements and Learning Plans were in place for IT Security staff.

The audit team also identified areas where management practices and processes should be improved.

Although the Departmental Security Plan defines an appropriate governance structure, oversight should be strengthened through a more effective use of these governance bodies, as senior management may not have a fulsome view of significant IT security planning issues and risks which could result in business objectives not being achieved.

While we found components of an IT security strategy and plan, they were not sufficiently integrated and aligned to provide for a well-defined and comprehensive IT security strategy. Additionally, even though individual Threat Risk Assessments are done on specific projects, there is no comprehensive IT security risk assessment

Despite the lack of a complete IT security internal control framework or list of controls including their criticality and risk, specific applications including their respective list of key processes were appropriately certified. As a more robust internal control framework is developed, controls and their related monitoring requirements should be strengthened in the areas of; user access, configuration management, IT asset tracking and event logging.

More regular training and awareness activities as well as communication of IT security processes and procedures would be beneficial for the department as a whole to ensure comprehensive coverage of key IT security responsibilities.

1.7 Summary of Audit Recommendations

Under the direction of the Assistant Deputy Minister, Corporate Management Branch, the CIO should:

1. Clearly define and document an overall IT security strategy or plan, aligned with the DSP, and report to the DMC on progress.
2. Reinforce the governance structures currently in place to facilitate effective oversight of IT security.
3. In consultation with the DSO, ensure that a comprehensive IT security risk management process is developed and implemented.
4. Ensure that a comprehensive IT security control framework is developed, approved and implemented.
5. Ensure that appropriate risk-based monitoring processes are developed and implemented, specifically as it relates to user access, event logging, configuration management, and inventory management.
6. Ensure that the IT security roles and responsibilities shared between SSC and PS staff are further clarified.
7. Ensure that relevant and consistent IT security awareness/orientation sessions are regularly offered to PS staff, and that all relevant IT Security policies, directives, and standards are made available on InfoCentral.

1.8 Management Response

The Audit of Information Technology Security recognizes the criticality of IT as a strategic asset and critical enabler of departmental business services and the role of IT Security in the preservation of the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information. While CIOD's IMIT Security program leads and coordinates IT Security activities for Public Safety Canada, we all have a crucial role to play in helping to ensure our information and IT assets are protected in a manner commensurate with our role as a lead security agency in the Government of Canada (GC).

We appreciate the opportunity to work with our Audit partners in this audit of our IM/IT Security program in Public Safety Canada, as we understand we have a common goal of continuous improvement of our IT Security program. We are encouraged by the recognition that "… there are adequate and effective mechanisms in place to ensure the appropriate management of IT security…" but acknowledge that improvements can be made.

We fully accept all of the recommendations; the recommendations focus on reviewing and updating our policies, processes and procedures, the governance model, and oversight as well as clearly articulating the necessity of having regular reporting of IM/IT Security to departmental senior management. We recognize the benefit of these activities as they will reinforce our program, enhance our visibility and emphasize the importance of a vibrant, responsive IM/IT Security program to the entire department.

Approved By:

Rosemary Stephenson
Chief Audit Executive

2.0 Background

The audit of Information Technology (IT) Security was approved by the Deputy Minister on May 31, 2011 as part of the updated Risk-Based Internal Audit Plan 2011-12 to 2013-14.

Information Technology is a Strategic Asset and Critical Enabler of the Government of Canada's commitment to deliver integrated and easily accessible services to Canadians, while ensuring that internal administrative operations are managed efficiently and effectively. The Treasury Board (TB) *Policy on Government Security* defines IT Security as the "safeguards" to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information.

In 2005, the Treasury Board Secretariat (TBS) requested that all departments implement by December 2006 the *Management of Information Technology Security Standard* (MITS). This standard represents the baseline IT security standards for all Government of Canada departments to follow.

In 2011-12 the IT environment across the federal government went through significant changes in the delivery of IT services. Shared Services Canada (SSC) was created as the vehicle for network, server infrastructure, telecommunications and audio/video conferencing services for the forty-three departments and agencies with the largest IT spend in the Government of Canada. Formal Business Arrangement agreements were put in place with each department, and underline the fact that departmental service levels would continue to be met.

Roles and Responsibilities

As per the TB *Policy on Government Security* issued under section 7 of the *Financial Administration Act* (FAA), Deputy heads are accountable for the effective implementation and governance of security and identity management within their departments and share responsibility for the security of government as a whole.

MITS describes roles and responsibilities for key positions, including the department's Chief Information Officer (CIO) who is responsible for ensuring the effective and efficient management of the department's information and IT assets. Additionally departments must appoint an IT Security Coordinator (ITSC) with at least a functional reporting relationship to both the departmental CIO and the Departmental Security Officer (DSO).

Currently, roles and responsibilities for IT security are delineated between SSC and the CIOD and DSO, both of which are within the Corporate Management Branch.

The CIOD is responsible for:

- Overall management of, and reporting on, the departmental IM/IT Security program,
- Communications Security,
- Management of the Top Secret and Classified Networks,
- Implementation of the departmental IM/IT Security Risk Management program,
- Administration of an ongoing training and awareness program to inform all personnel of their IM/IT Security policy compliance responsibilities,
- Help Desk which manages the IT security incidents,
- IT Security Incident management,
- Providing IM/IT Security content into corporate documents.

The DSO is responsible for:

- Establishing and directing the departmental security program,
- Managing the overall security risks which include planning, monitoring and oversight, performance measurement and evaluation.

SSC is responsible for:

- Managing all aspects of the departmental e-mail systems, secret and protected B networks, server infrastructure and data centre.

2.1 Audit Objective

The objective of the audit was to assess the department's compliance with the TB *Policy on the Management of Information Technology* and the *Policy on Government Security*, focusing on IT security aspects and requirements. This included assurance that internal controls over the management of IT security were adequate and effective.

2.2 Audit Criteria and Scope

The audit period covered the timeframe from January 1, 2012 to June 30, 2012.

The audit scope was determined based on the following parameters:

- Higher priority IT security risks that would bring value to the department
- Areas where controls are under the purview of PS (versus SSC)
- Availability of audit resources

The scope of the audit included the following key areas:

- IT Security Planning
- IT Security Strategy and Governance
- IT Security Monitoring
- IT Security Risk Management
- IT Security Roles and Training
- System Configuration

- IT Security Management
- Incident and problem management

Where applicable, the test of controls was done only as they relate to the Protected B network.

The detailed audit criteria are listed in Appendix A.

2.3 Approach

This internal audit used relevant criteria to assess whether the management control framework to manage IT security were adequate and effective. The audit criteria was derived from TB policies, the *MITS* standard and ISACA's *Control Objectives for Information and Related Technology (COBIT 5)*.

Procedures for gathering evidence included interviews as well as a review of records and an examination of selected documentation, such as threat and risk assessments, vulnerability assessments, statements of sensitivity, privacy impact assessments, policies, standards, guidelines, service level agreements, frameworks and plans.

The application of these procedures was intended to allow the formulation of a conclusion as to whether the established audit criteria have been met. Standards for evidence included ensuring that the information was sufficient, reliable, relevant, and useful to draw conclusions. The audit also identified recommendations to address priority areas for improvement.

2.4 Audit Opinion

In my opinion, there are adequate and effective mechanisms in place to ensure the appropriate management of IT security, although some important areas require management attention to address some residual risk exposure.

2.5 Findings, Recommendations and Management Response

Governance and Planning

Governance

The audit expected to find an appropriate IT security governance framework that provides for unambiguous accountability, confirms delivery of the IT security strategies and objectives, and ensures reporting on IT security status and issues.

The audit found that the Departmental Security Plan (DSP) identifies a formal governance structure which is integrated into the corporate governance structure. Specifically, it identifies the Deputy Minister and the Associate Deputy Minister as responsible overall; however it further notes that decision-making, exercising controls and accountabilities for all its activities, including corporate security, are governed by the Departmental Management Committee (DMC) and Executive Committee (EXCOM). Working groups and committees also support DMC in

decision-making related to corporate security, such as the Departmental Security Committee (DSC), the Planning and Reporting Network/Committee, the DG IT Steering Committee and the Business Continuity Planning working group.

The DSC is co-chaired by the Director General of Corporate Services and the CIO and is expected to meet on a bi-monthly basis in order to provide; direction, timely and effective oversight, advice, and guidance to PS's Corporate Security Program. However, only one DSC meeting took place this calendar year and while IT security may have been discussed, there were no IT security items on the agenda, or in the record of decisions.

Further, while the DG IT steering Committee, through its co-chairs, is expected to report to the DMC on a quarterly basis on progress against approved priorities and to seek decisions, there were no IT security agenda items on DMC or EXCOM during the audit period.

Given the limited discussion concerning IT security, management may not be up to date on IT security priorities and risks.

Planning

The audit expected to find an overall IT security plan that takes into consideration the IT infrastructure and the security culture, and that the organization ensures that the plan is aligned with security policies and procedures, together with appropriate investments in services, personnel, software and hardware, and that security policy and procedures are communicated to stakeholders and users.

The auditors found that a set of IT security policies, directives and standards were in place, and align with government and industry frameworks, policies and best practices. However, we are unclear as to the accountability for the policy lifecycle management.

The audit examined the CIOD 2010-2015 Strategic Plan, the CIOD 2012-2013 IT Plan as well as the 2010-2013 DSP looking for the department`s overall IT security strategy and or plan.

- The CIOD 2010-2015 Strategic Plan outlines five strategic goals, none of which is specific to IT security.
- The CIOD 2012-2013 IT Plan is composed of the same five strategic goals identified in the Strategic Plan and 31 IT projects, some of which relate to IT security. There is also an IM/IT security section, however it is unclear how this section aligns with the rest of the document.
- The DSO 2010-2013 DSP describes PS's Corporate Security Program, it is not intended to be IT focused. This plan identifies corporate security priorities, one of which is related to IT security.

While components of the IT security strategy and plan were found amongst the various documents, the auditors were unable to determine the specific IT security strategy or plan for PS. Further it is unclear how IT security priorities are identified and aligned between the DSP, the

CIOD Strategic Plan, and the CIOD IT Plan, as there is not always a clear linkage between the priorities, strategic goals, plans, objectives, and projects.

Without a well-defined and aligned IT security strategy or plan (whether one document or several), there is a risk that the department may not be focused on the right IT security activities to meet departmental requirements and business objectives and to ensure investments are well founded.

Recommendations:

Under the direction of the Assistant Deputy Minister, Corporate Management Branch:

1. The CIO should clearly define and document an overall IT security strategy or plan, aligned with the DSP, and report to the DMC on progress.
2. The CIO should reinforce the governance structures currently in place to facilitate effective oversight of IT security.

Management Action Plan	
Management Action Plan	**Planned Completion Date**
Review the DSP and provide IT security input as required.	Q1 2013-14
Develop a 5-year IT Security Strategic Plan and roadmap for integration into the 5-year CIOD Strategic Plan.	Q1 2013-14
Develop an annual IT Security plan for incorporation into the annual CIOD IT Plan which is submitted to TBS.	Q1 2013-14
Incorporate IT Security information on CIOD Quarterly dashboard.	Q2 2013-14
Develop a proposed plan for regular and ad hoc IT Security reports to DMC.	Q2 2013-14
Review current governance bodies, IT Security responsibilities and reporting requirements.	Q1 2013-14
Update TORs as required, standing agenda items and regular reporting for IT Security.	Q1 2013-14

2.5.2 Risk Management

The audit expected to find an IT security risk management process integrated with the departmental risk-management framework. The audit also expected that the committed actions are owned by the affected process owner(s) who would monitor the execution of the plans, and report on any deviations to senior management. IT security risks are identified in four main documents:

- The Corporate Risk Profile (CRP),
- The 2005 Departmental Security Threat and Risk Assessment (TRA),

- The Security Risk Register, and
- The System Specific TRA's.

These documents are developed by different groups within the department; the CRP is developed by the Strategic Policy branch; the Departmental Security TRA, developed in 2005, and the Security Risk Register are prepared by the DSO; and the system specific TRA's are prepared by the CIOD. Each uses different risk identification approaches.

The CIOD identifies IT security risks for specific systems or applications through their TRA process. The audit found this TRA process to be comprehensive; it was appropriately informed and used robust tools resulting in formal subject specific TRA reports. However, no management action plans were found which should have included the risk owners, schedules, risk mitigation activities, and costs and benefits.

The Departmental Security TRA and a security risk register were developed with the intention of having a comprehensive inventory of all the security risks existing within the department. However based on the date of the Departmental TRA (2005), the audit questioned the relevancy of this report given that no further update was done. The audit noted that the security risk register also had no corresponding risk mitigation action plans, assigned risk owners, timelines, or costs, nor did it include input from the CIOD. Further it was unclear how these security risks were integrated into the processes followed by the CIOD or the CRP. As a result the audit could not attest to whether the security risk registry was complete or aligned with other risks identified in the other above mentioned documents.

Overall there was no comprehensive IT security risk assessment that consolidated and correlated all relevant IT security risks. Given the vast number of IT security risks that currently exist, having a comprehensive IT security risk assessment would allow the CIOD to better manage, mitigate, and communicate high risk areas to appropriate individuals in a more efficient and structured approach.

Without a robust IT security risk management process and associated mitigation plans, high risk areas may not be appropriately identified, managed and communicated resulting in the potential materialization of risk.

Recommendation:

Under the direction of the Assistant Deputy Minister, Corporate Management Branch:

3. The CIO in consultation with DSO should ensure that a comprehensive IT security risk management process is developed and implemented.

Management Action Plan	
Management Action Plan	**Planned Completion Date**
Review current departmental risk management process for Corporate Risk Profile.	Q1 2013-14
Review current departmental security risk management process.	Q2 2013-14
Develop and implement an IT security risk management process that is consistent with the departmental security risk management process.	Q3 2013-14

2.5.3 IT security control framework

The audit expected to find in place an IT security control framework, based on risk, to assist in appropriately managing IT security risks to the department. It was also expected that the key controls within the framework were appropriately monitored. Further it was expected that the IT security controls would be independently assessed according to risk and business objectives, or if systems, services or risks changed significantly.

The audit was unable to find a complete risk-based IT security control framework or list of all key IT security internal controls that require managerial review and oversight; rather there were application specific control listings. For example the CIOD had a subset of IT security controls applicable to the Protected B network, which they had mapped to the draft Information Technology Security Guidance 33 (ITSG-33 [1]). However, the audit could not confirm that this list was comprehensive in nature, further it did not identify the controls by their criticality or frequency and methodology by which they should be monitored.

While the Protected B network was certified in 2011 and is expected to be re-certified in 2013, and the social media tool YAMMER was independently assessed in 2012, it is unclear if there are any other plans to verify the completeness and effectiveness of all relevant IT security controls.

Without a list of key IT security controls there is a risk that monitoring may not be effective in identifying and mitigating risks.

Recommendation:

Under the direction of the Assistant Deputy Minister, Corporate Management Branch:

4. The CIO should ensure that an IT security control framework is developed, approved and implemented and that IT security processes are monitored with regular reporting.

Management Action Plan	
Management Action Plan	**Planned Completion Date**
Review current departmental IT security control framework, including processes.	Q1 2013-14
Update departmental security assessment procedures to require the identification of appropriate controls as part of the initial stage of each security assessment.	Q2 2013-14
Update monitoring and reporting on IT security processes.	Q3 2013-14
Document process for continuous update and validation of IT security control framework and processes.	Q3 2013-14

2.5.4 Key IT security management activities

User Access

The audit expected to find that all users (internal, external and temporary) and their IT activities (business application, IT environment, system operations, development and maintenance) are approved, uniquely identifiable, maintained in a central repository, and appropriately reviewed and validated to ensure continued integrity.

User identification and access rights are managed through the Active Directory system within the Microsoft Windows operating system. Employees are defined as either general users (GUs) or system administrators (SAs). SAs generally have more access within the network and are reserved for IT personnel. GUs normally have restricted access and are for non IT personnel. If properly set, the auditing tools part of the Active Directory and other similar tools are able to track IT activity performed by various network users.

In some instances generic accounts are created within SA and GU categories which are not assigned to a unique individual and may have multiple users. These generic accounts are generally used for special circumstances, e.g. emergency response situations. While there are legitimate reasons for generic accounts it becomes more difficult to monitor them for security purposes.

The Active Directory had 2,632 accounts, out of these accounts, the auditors were able to identify that approximately 15-25% were generic accounts (GU or SA) and that 68 were uniquely identifiable SA accounts. We were concerned with the number of both generic and SA accounts especially given the difficulty monitoring generic accounts, and the fact that SA and generic accounts are not consistently approved according to departmental procedures. These observations were provided to CIOD who have begun to review these accounts.

The audit found that systems are configured to enforce user authentication before access is granted. Further the requirements for passwords are defined in the Network Password Standard and Procedures and enforced accordingly.

The audit found that user accounts and access rights, both GUs and SAs, are not being reviewed by management on a regular basis. For example: several active user accounts, including SA accounts were assigned to individuals who were no longer employed at PS; no compensating controls (e.g., management monitoring) exist for user accounts with segregation of duties issues; etc.

Without robust user account management procedures the department is at risk of access control violations and security breaches.

Event monitoring, virus protection, and security patches

The audit expected to find appropriate preventive, detective and corrective measures in place to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam). Further the audit expected to find that the IT activity logging is enabled and the logs are monitored to enable the prevention and/or timely detection and reporting of unusual and/or abnormal activities.

The audit found that measures are in place to verify that all network devices are at current release and security patch levels. Additionally security barriers are strategically placed at the network's perimeter, between the department's trusted internal network and non-trusted public (i.e., Internet), vendor (i.e., service organization) or business partner (i.e. extranet) segments thereby protecting PS from external threats. The audit also found that automated tools have been implemented to provide protection against viruses and to ensure that violations are appropriately communicated. The virus protection tool has been installed on workstations and includes virus definition files that are centrally updated on a regular basis. This tool scans downloaded files from the Internet for vulnerabilities before being allowed into the network. The CIOD uses security tools to routinely monitor the network for security events, defined as abnormal activity.

In regard to the security logging function, the audit found that PS has a tool which logs IT network activity. However the audit noted some weaknesses:

- not all devices are reporting events e.g. PS workstations,
- no central repository exists, audit data is stored in many locations, and are subject to discretionary deletion, and
- there are no regular reviews of audit logs; they are actioned only when the logging tool indicates a potential incident.

The impact of not having a robust logging and log monitoring function creates a risk of undetected potential incidents, and does not allow timely corrections, and potential necessary monitoring adjustments.

System Configuration

The audit expected to find that configuration management (CM) was in place. CM is the detailed recording and updating of information that describes an organizations hardware and software. This includes management and logging of all changes to the configuration repository, and

periodic review of the configuration data to verify and confirm the integrity of the current and historical configuration.

The audit found some elements of CM were in place. For example the ClOD has developed a configuration policy requiring that configuration items and their attributes be identified and maintained, and that change, configuration, and release management are integrated. In addition, there is a Change Configuration Board (CCB) that discusses and approves change configuration requests. CCB meetings take place on a regular basis and only authorized personnel have designated access to the change configuration items. However, the audit found that the CCB does not monitor the approved configuration changes to ensure changes were implemented as intended and they addressed the issue. When configuration baselines for components, including those related to IT security, are not approved and periodically reviewed afterwards, there is a risk that unauthorized changes to hardware and software are not discovered, or that authorized changes are not being made, leaving the networks exposed to security breaches.

Further, the audit found that there is no centralized repository that would identify all configuration items and their attributes or a process that identifies and ensures the integrity of all critical configuration items. However baseline configurations and change configurations can be found in standalone documents and in the CCB SharePoint application. Without a central repository of all approved configuration items, CM is cumbersome and may be incomplete which could lead business disruptions.

IT Asset Inventory Management

The audit expected to find a current and complete IT asset inventory. Inventory management is essential to ensure that key assets such as laptops, desktop computers, mobile devices, and secret network hubs are not misplaced or lost.

The audit found that there is no internal policy in place for physical IT asset tagging and that some assets sampled during the audit were not tagged appropriately. These results indicated that the IT asset inventory is not up-to-date, complete, nor in some cases accurate.

Not having an IT asset tagging policy in place or an up-to-date IT asset inventory may lead to misused or stolen assets leading to a potential security breach.

Recommendation:

Under the direction of the Assistant Deputy Minister, Corporate Management Branch:

5. The CIO should ensure that appropriate risk-based monitoring processes are developed and implemented, specifically as they relate to user access, event logging, configuration management, and IT asset inventory management.

Management Action Plan	
Management Action Plan	**Planned Completion Date**
Review and update account management process including regularized reviews and reporting.	Q1 2013-14
Review and update admin account management process, including regularized reviews and reporting.	Q1 2013-14
Review and update generic account management process including regularized reviews and reporting.	Q1 2013-14
Review and update logging capabilities if required, including event logging on a daily basis and options for specific circumstances.	Q2 2013-14
Review configuration management process, including CCB, and impact of creating and managing a centralized repository including regularized reviews and reporting.	Q2 2013-14
Review and update IT asset inventory management process, including regularized reviews and reporting.	Q1 2013-14

2.5.5 Roles, Responsibilities, and Training

Roles and Responsibilities

The audit expected to find that roles and responsibilities of IT security personnel are established and communicated.

The audit found that roles and responsibilities specific to PS are established, communicated, and understood. As well, Performance Agreements, which included expectations that linked up to objectives, and up-to-date learning plans are completed regularly for IT Security staff.

As it pertains to the delineation of roles and responsibilities between SSC and PS, the audit found there was less clarity and understanding. While there is a collegial working relationship between them and a formal Business Arrangement agreement is in place, it does not provide detailed responsibilities.

By not having well defined roles and responsibilities between SSC and PS, which are key controls, there is a risk of misalignment.

Training and Awareness

The audit expected to find that employees had sufficient training, awareness and understanding of their IT security responsibilities.

The audit found that CIOD communicates to appropriate stakeholders and users throughout the department on an adhoc basis about relevant IT Security activities.

CIOD has also developed IT security policies and procedures however not everything is readily available for PS staff, for example the Directive on IT Security which identifies overall roles and responsibilities, is not on Infocentral, nor are all of the IT Security Standards. CIOD is aware and has plans to address this issue.

The department has various training and awareness activities that include components of IT security however the audit found that these activities were not mandatory or scheduled on a timely basis, nor is it clear whether these activities provide comprehensive coverage of key IT security responsibilities.

A lack of sufficient awareness and understanding of IT security could result in policy violations, non-compliance with policy and security breaches.

Recommendations:

Under the direction of the Assistant Deputy Minister, Corporate Management Branch:

6. The CIO should ensure that the IT security roles and responsibilities shared between SSC and PS staff are further clarified.
7. The CIO should ensure that relevant and consistent IT security awareness/orientation sessions are regularly offered to PS staff, and that all relevant IT Security policies, directives, and standards are made available on InfoCentral.

<table>
<tr><td colspan="2">Management Action Plan</td></tr>
<tr><th>Management Action Plan</th><th>Planned Completion Date</th></tr>
<tr><td>Review, update and document departmental IT Security roles and responsibilities.</td><td rowspan="3">Must be reviewed and/or updated in context of SSC re-org and potential or planned change in roles and responsibilities</td></tr>
<tr><td>Allocate roles and responsibilities to ensure all IT Security activities are aligned.</td></tr>
<tr><td>Define a regular review and update to ensure organizational changes are accounted for and clarity is maintained.</td></tr>
<tr><td>Develop an IT Security Awareness and Training Strategic Plan and roadmap.</td><td>Q1 2013-14</td></tr>
<tr><td>Develop the first annual IT Security Awareness and Training plan.</td><td>Q2 2013-14</td></tr>
<tr><td>Review departmental IT security policy instruments to ensure compliance with current GC directions; update if required and identify gaps.</td><td>Q4 2013-14</td></tr>
</table>

Appendix A – Audit Criteria

The following criteria were assessed:

IT Security Planning

There is an overall IT security plan in place that takes into consideration the IT infrastructure and the security culture, and the organization ensures that the plan is aligned with security policies and procedures together with appropriate investments in services, personnel, software and hardware, and that security policies and procedures are communicated to stakeholders and users.

IT Security Strategy and Governance

An IT security governance framework is defined, established and aligned with the IT governance framework, and the overall enterprise governance and control environment.

The IT security governance framework is based on a suitable IT security process and control model and provide for unambiguous accountability and practices to avoid a breakdown in internal control and oversight.

The IT security governance framework ensures compliance with laws and regulations and is aligned with, and confirms delivery of, the enterprise's strategies and objectives.

IT security governance status and issues are reported on.

A set of policies to support the IT security strategy is developed and maintained, and their relevance is confirmed and approved regularly.

IT Security Monitoring

The IT security control environment and control framework to meet organizational objectives is continuously monitored, benchmarked and improved.

Further assurance of the completeness and effectiveness of IT security related internal controls through third-party reviews is obtained.

IT Risk Management

An IT security risk management framework, as part of the IT security management framework, is established that is aligned to the department's risk management framework.

Ownership and responsibility for IT security-related risks within the department is embedded at an appropriate senior level, and roles critical for managing IT risks, including the specific responsibility for information security, physical security and compliance, are defined and assigned.

The likelihood and impact of all identified IT security risks is assessed on a recurrent basis using qualitative and quantitative method, and if the likelihood and impact associated with inherent and residual risk is determined individually, by category and on a portfolio basis.

The control activities are prioritized and planned at all levels to implement the risk responses identified as necessary, including identification of costs, benefits and responsibility for execution.

The approval for recommended actions is obtained and any residual risk is accepted. The committed actions are owned by the affected process owner(s) who would monitor the execution of the plans, and report on any deviations to senior management.

IT Security Roles and Training

Roles and responsibilities for IT personnel, including IT security personnel, and end users that delineate between IT personnel and end-user authority, responsibilities and accountability for meeting the organization's needs are established and communicated.

Key IT security personnel (e.g., replacements/backup personnel) are defined and identified, and reliance on a single individual performing a critical job function is minimized.

Awareness and understanding of business and IT security objectives and direction is communicated to appropriate stakeholders and users throughout the enterprise.

A curriculum for each target group of employees is established and regularly updated considering current and future business needs and strategy; value of information as an asset; corporate values (ethical values, control and security culture, etc.); implementation of new IT infrastructure and software (i.e., packages, applications); current and future skills, competence profiles, and certification and/or credentialing needs as well as required reaccreditation; delivery methods (e.g., classroom, web-based), target group size, accessibility and timing.

IT and IT security employees are provided with appropriate orientation when hired and ongoing training to maintain their knowledge, skills, abilities, internal controls and IT security awareness at the level required to achieve organizational goals.

System Configuration

Configuration procedures are established to support management and logging of all changes to the configuration repository.

The configuration data is periodically reviewed to verify and confirm the integrity of the current and historical configuration.

Installed software is periodically reviewed against the policy for software usage to identify personal or unlicensed software or any software instances in excess of current license agreements, and errors and deviations are reported and acted on and corrected.

Security Management

IT security is managed at the highest appropriate organizational level, so the management of security actions is in line with business requirements.

The organization ensures that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable, and enables user identities via authentication mechanisms.

The organization maintains user identities and access rights in a central repository.

The organization confirms that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities, and ensures that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person.

The organization addresses requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures which includes an approval procedure outlining the data or system owner granting the access privileges. These procedures apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. The organization performs regular management review of all accounts and related privileges.

The IT security implementation is tested and monitored in a proactive way, and is reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained.

The logging and monitoring function enables the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed. Security-related technology is made resistant to tampering, and prevents the unnecessary disclosure of security documentation.

Preventive, detective and corrective measures are put in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).

Security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) are used to authorize access and control information flows from and to networks, and if firewall rules fail to reflect the organization's security policy.

Incident and Problem Management

A help desk function, which is the user interface with IT, to register, communicate, dispatch and analyze all calls, reported incidents, service requests and information demands is established.

There are monitoring and escalation procedures in place based on agreed-upon service levels relative to the appropriate SLA that allow classification and prioritization of any reported issue as an incident, service request or information request.

A function and system to allow logging and tracking of calls, incidents, service requests and information needs is established. Incidents are classified according to a business and service priority and routed to the appropriate problem management team, where necessary. Customers are kept informed of the status of their queries with all incidents being tracked.

The characteristics of potential security incidents are clearly defined and communicated so they can be properly classified and treated by the incident and problem management process.

Help desk procedures are established, so incidents that cannot be resolved immediately are appropriately escalated according to limits defined in the SLA and, if appropriate, workarounds are provided. The organization ensures that incident ownership and life cycle monitoring remain with the help desk for user-based incidents, regardless which IT group is working on resolution activities.

Procedures for the monitoring of timely clearance of customer queries are established. When the incident has been resolved, the organization ensures that the help desk records the resolution steps, and confirm that the action taken has been agreed to by the customer, and that a record and report of unresolved incidents (known errors and workarounds) are kept to provide information for proper problem management.

Reports of service desk activity are produced to enable management to measure service performance and service response times and to identify trends or recurring problems, so service can be continually improved.

The related processes of configuration, incident and problem management are integrated to ensure effective management of problems and enable improvements.

Appendix B – Applicable policies, legislation and regulations

1. Treasury Board (TB)
    - Audit Criteria Related to the Management Accountability Framework: A Tool for Internal Auditors, March 2011 – Unpublished
    - Policy on Internal Control
    - Policy on Government Security (PGS)
    - Policy on the Management of Information Technology
    - Directive on the Management of Information Technology
    - Operational Security Standard on Physical Security
    - Operational Security Standard on Business Continuity Planning Program
    - Operational Security Standard: Management of Information Technology Security (MITS)
    - Personnel Security Standard
    - Security Organization and Administration Standard
    - Security and Contracting Management Standard
    - Information Technology Security Audit Guide (archived)
    - Policy for Public Key Infrastructure Management in the Government of Canada (archived)
    - Policy on Internal Audit
    - Guideline on the Management of Public Key Infrastructure in the Government of Canada
2. Other Government Organizations
    - RCMP guide on Physical Protection of Computer Servers
    - Communications Security Establishment (CSE) guides:
        - ITSG-04 Harmonized TRA Methodology
        - ITSG-06 Clearing and Declassifying Data Storage Devices
        - ITSG-22 Baseline Security Requirements for Network Security Zones in the Government of Canada
        - ITSG-33 IT Security Risk Management: A Lifecycle Approach
3. Other Non-Government Organizations
    - ISACA/ITGI Control Objectives for Information and related Technology (COBIT® 5)
    - The IIA Global Technology Audit Guides (GTAGs)
        - GTAG 1: Information Technology Controls
        - GTAG 2: Change and Patch Management Controls: Critical for Organizational Success
        - GTAG 4: Management of IT Auditing
        - GTAG 6: Managing and Auditing IT Vulnerabilities
        - GTAG 7: Information Technology Outsourcing
        - GTAG 9: Identity and Access Management
        - GTAG 10: Business Continuity Management
        - GTAG 11: Developing the IT Audit Plan
        - GTAG 12: Auditing IT Projects
        - GTAG 15: Information Security Governance

Appendix C – Audit Activities

The audit included the following activities:

- Interviews
- Examination of selected documentation, such as threat and risk assessments, vulnerability assessments, statements of sensitivity, privacy impact assessments, policies, standards, guidelines, service level agreements, frameworks and plans
- Testing of selected transactions and validation of their accuracy for the period January 1, 2012 to June 30, 2012
- Effectiveness testing of internal control processes

Footnotes

1.

ITSG-33 was developed by Communications Security Establishment Canada to help departments ensure security is considered from the start. Following ITSG-33 principles helps ensure predictability and cost-effectiveness. ITSG-33, aligned with MITS and the TB policies, describes the roles, responsibilities and activities that help departments manage IT security risks.

ITSG-33 contains a catalogue of Security Controls structured into three classes of control families: Technical, Operational and Management, representing a holistic collection of standardized security requirements that should be considered and leveraged when building and operating IT environments. Adhering to ITSG-33 should aid departments reap significant benefits including: compliance with the overall risk management strategy and objectives established by TBS; assurance that all aspects of IT security are addressed in an efficient manner; and predictability and cost-effectiveness with regards to IT security risk management.

Date modified
2013-08-19