Canada's Nuclear Regulator

Audit of CNSC's Management of Information Technology and Telecommunications Assets

Office of Audit and Ethics

Recommended by the Audit Committee on November 21, 2016

Approved by the President on February 27, 2017

e-Doc 4957453-docx

e-Doc 5191476-pdf

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Canada

Table of Contents

Executive Summary

Background

This report was revised on February 8, 2017. It includes the management action plans which address the audit recommendations.

Section 62 of the *Financial Administration Act* requires the deputy head of every department to maintain adequate records in relation to public property for which the department is responsible and to comply with regulations of the Treasury Board governing the custody and control of public property. All federal departments and agencies must ensure sound stewardship over the funds provided to them and demonstrate value for money in procuring, managing and using assets and services. Part of this stewardship responsibility is the requirement for departments to implement appropriate and effective internal controls and management practices to ensure that the assets purchased with its resources are accounted for and protected from unauthorized use, damage, or loss.

In 2012, the Government of Canada (GC) began a major transformation with respect to the management of information technology (IT) assets and delivery of IT services. The transformation began with the creation of Shared Services Canada (SSC). SSC's mandate is to provide the 43 federal departments and agencies with core IT services (email, data centre and telecommunications). SSC also provides non-core, or optional, IT services to departments and agencies on a cost-recovery basis. SSC now manages the GC's computer network and processing services, and owns the GC IT hardware and software assets classified as capital. Similarly, IT assets related to telecommunications services, which include both landline and mobile telephones, have been transferred to SSC.

As a cost-recovery agency, the Canadian Nuclear Safety Commission (CNSC) has negotiated with SSC an annual transfer of funds for the delivery of both core and optional IT services. Under the arrangement, the CNSC is responsible for managing only desktop computing, which includes hardware and non-core software. SSC is responsible for managing all other IT assets and services, including data centres, network infrastructure, processing systems and software, and core desktop software (operating system and office productivity suite).

IT asset management at the CNSC has been the focus of previous audits by the Office of Audit and Ethics (OAE). It has resulted in a number of recommendations to strengthen controls. The following audits were issued by the OAE:

- *Audit of IT Asset Management Report*, July 10, 2012

- *Audit of Mobile Telecommunication Devices*, July 10, 2012.

Objectives and scope

The objectives of the audit were to provide reasonable assurance to CNSC management that:

- adequate and effective IT asset management processes and controls are in place for assets both owned by and entrusted to the CNSC, in order to maintain the integrity of the IT assets while meeting the CNSC's and GC's requirements
- IT assets inventory and records are complete and accurate

The Treasury Board Policy on Information Technology defines information technology to include "any equipment or system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It includes all matters concerned with the design, development, installation, and implementation of information systems and applications to meet business requirements."

This audit includes all the IT and telecommunications assets listed in appendix D.

Audit fieldwork was conducted from March to October 2015.

Summary of observations

- *Governance structure*

  A management structure for IT assets is implemented, but the IT service management framework has yet to be defined for IT assets entrusted to the CNSC.

- *Roles and responsibilities*

  The Information Management and Technology Directorate (IMTD) understands its roles and responsibilities for managing CNSC IT assets, but some incompatible roles exist. For the management of IT services, roles and responsibilities are not documented.

- *Policy development*

  Policy documents for the management of CNSC assets are not always published after changes are identified, reviewed, updated, approved and communicated. A procedure document for the management of IT services does not exist.

- *Processes and procedures*

  Effective processes are in place for CNSC asset planning with respect to acquisition, replacement and disposal of IT assets, but procedures are not documented for acquisition of IT assets. Improvements are required before the disposal of IT assets is properly controlled.

- *Compliance with Treasury Board policies*

  IMTD processes comply with CNSC and Treasury Boards policies on acquisition and disposal of IT assets.

- *Procurement practices*

  IMTD has implemented an effective procurement standard to control IT asset procurement.

- *Employees benefiting from process*

  Improvements must be made to the roles and responsibilities; and access to valuable assets, including those slated for destruction, must be restricted.

- *Systems for recording and tracking*

  An asset tracking system is in place and access is properly controlled. However, improvements are required for:

  - the process for tagging assets
  - eliminating a duplicate asset tracking system
  - removing SSC assets from the hardware spreadsheet used for inventory tracking

- *Accuracy of CNSC records*

  IT hardware asset records are not always accurately reflected in the IT asset management system:

  - Material computer asset records are accurate.
  - Other IT hardware asset records are not accurate; the verification process does not ensure that they are being counted.
  - IT software asset records are not being verified; completeness and accuracy cannot be determined.

- *Inventory safeguarding and disposal*

IT assets are properly safeguarded when not in service or scheduled for destruction. IT assets identified for disposal follow the TB disposal directive requirements and are properly removed from the tracking system.

- *Software Verification*
  There is no assurance that the software installed does not exceed the licences owned by the CNSC.

Overall conclusion

There is an established management framework in place, designed to promote general oversight, accountability, risk management and control over IT assets. However, there are a number of areas in which further enhancements to mechanisms, practices and controls will be required. In addition, the management framework for telecommunications services procured from SSC needs to be developed and implemented.

The audit found that material IT hardware asset records were accurate and reliable, but lower dollar value items had a higher degree of inaccuracy. For software assets, the accuracy and reliability of the information could not be assessed, as there was no mechanism in place to verify the installed software.

The audit team would like to acknowledge and thank management for its support throughout the conduct of this audit.

1 Introduction

1.1 Background

Section 62 of the *Financial Administration Act* requires the deputy head of every department to maintain adequate records in relation to public property for which the department is responsible and to comply with regulations of the Treasury Board governing the custody and control of public property. All federal departments and agencies must ensure sound stewardship over the funds provided to them and demonstrate value for money in procuring, managing and using assets and services. Part of this stewardship responsibility is the requirement for departments to implement appropriate and effective internal controls and management practices to ensure that the assets purchased with its resources are accounted for and protected from unauthorized use, damage, or loss.

In 2012, the Government of Canada (GC) began a major transformation with respect to the management of information technology (IT) assets and delivery of IT services. The transformation began with the creation of Shared Services Canada (SSC). SSC's mandate is to provide the 43 federal departments and agencies with core IT services (email, data centre and telecommunications). SSC also provides non-core, or optional, IT services to departments and agencies on a cost-recovery basis. SSC now manages the GC's computer network and processing services, and owns the government IT hardware and software assets classified as capital. Similarly, IT assets related to telecommunications services, which include both landline and mobile telephones, have been transferred to SSC.

As a cost-recovery agency, the Canadian Nuclear Safety Commission (CNSC) has negotiated with SSC an annual transfer of funds for the delivery of both core and optional IT services. Under the arrangement, the CNSC is responsible for managing only desktop computing, which includes hardware and non-core software. SSC is responsible for managing all other IT assets and services, including data centres, network infrastructure, processing systems and software, and core desktop software (operating system and office productivity suite).

IT asset management at the CNSC has been the focus of previous audits by the Office of Audit and Ethics (OAE). It has resulted in a number of recommendations to strengthen controls. The following audits were issued by the OAE:

- *Audit of IT Asset Management Report*, July 10, 2012
- *Audit of Mobile Telecommunication Devices*, July 10, 2012.

1.2 Authority

The audit of the CNSC's management of IT and telecommunications assets was part of the approved CNSC *Risk-Based Audit Plan* for the period 2015–16 to 2017–18.

1.3 Objectives and scope

The objectives of the audit were to provide reasonable assurance to CNSC management that:

- adequate and effective IT asset management processes and controls are in place for assets both owned by and entrusted to the CNSC, in order to maintain the integrity of the IT assets while meeting the CNSC's and GC's requirements
- IT assets inventory and records are complete and accurate

The Treasury Board Policy on Information Technology defines information technology to include "any equipment or system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It includes all matters concerned with the design, development, installation, and implementation of information systems and applications to meet business requirements."

This audit includes all the information technology and telecommunications assets listed in appendix D.

Audit fieldwork was conducted from March to October 2015.

1.4 Analysis of risks

During the audit's planning phase, an analysis was conducted to identify the potential risks faced by the audit entity, and to evaluate and prioritize their relevance to the audit objective. Risks were identified by reviewing governing policy, previous OAE audit working papers, and recent audits conducted on similar areas within the federal government on similar areas.

The following areas of inherent risk and exposure were identified for examination during the audit:

- procedures for managing the IT asset lifecycle may not be adequate or are not being properly carried out
- the CNSC's governing directives and guidelines may not be adequate, reflect TB direction or result in appropriate practices

- records do not accurately reflect CNSC-owned IT assets and IT assets entrusted to CNSC employees

1.5 Audit criteria

Appendix a provides the lines of enquiry and related audit criteria used to achieve the audit objectives.

1.6 Approach and methodology

During the audit's examination phase, the audit team:

- reviewed CNSC policies, directives, standards, and procedures to assess alignment with relevant TB policies with respect to IT assets.conducted interviews with CNSC staff responsible for the management of the CNSC's owned IT assets and the management of IT assets entrusted to the CNSC, to obtain information on processes, procedures and documentation for the areas of concern
- assessed the information gathered and collected evidence to identify potential opportunities for improvement
- reviewed controls for ensuring required IT assets entrusted to the CNSC are being provided and delivered by SSC
- conducted a complete inventory count of IT assets to assess the accuracy of IT asset record.

The audit findings represent the processes and practices in place between March and October 2015. Audit findings were discussed with CNSC management prior to their finalization.

1.7 Statement of conformance

This audit conforms to the *Internal Auditing Standards for the Government of Canada*, as supported by the results of the OAE quality assurance and improvement program.

2 Audit observations and recommendations

2.1 Line of enquiry 1 - Management control framework

This line of enquiry assesses the governance and oversight structures in place to ensure that IT assets – owned and/or consumed by the CNSC – are managed appropriately and comply with GC and CNSC policies.

2.1.1 Governing policies, directives and procedures

The audit examined the extent to which governing policies, directives and procedures are in place, adequate, and properly implemented. The audit identified relevant sources of legislation, TB policies, CNSC policies, directives, standards, and procedures with respect to IT assets both owned and/or entrusted to the CNSC.

The audit team found that the CNSC had a management of information technology policy. The policy contains one paragraph about managing the lifecycle of IT assets, which covers planning, procuring, operating, maintaining, retiring and disposing of IT assets. Also, the policy includes one paragraph on the management of IT services which states "IT services will be planned, available, consistent, secure, measured, managed, and supported". In support of the management of IT assets owned by the CNSC, the Information Management and Technology Directorate (IMTD) has implemented the Information Technology Asset Management Directive, which defines the expected behaviour of employees with respect to the use and safeguarding of IT assets owned by the CNSC, and covers the management practices in the IT asset lifecycle.

For telecommunications (voice) services, there is no equivalent directive or associated policies and procedures covering the key management activities being performed. IMTD indicated that:

- the management of telecommunications is under the full responsibility of SSC
- any directives or policies related to telecommunications are to be developed by SSC

We note that the Treasury Board Policy Framework for the Management of Assets and Acquired Services "sets the direction for the management of <u>assets and acquired services</u> to ensure the conduct of these activities provides value for money and demonstrates sound stewardship in program delivery. A failure to effectively manage these activities can result in increased program and administrative costs and can compromise program outcomes". More specifically, section 3.1 of the Treasury Board Policy on Management of Materiel states that: "Deputy heads are accountable to their respective minister and to the Treasury Board for the sound stewardship of the <u>materiel entrusted to them or used by their organization</u>".

The CNSC transferred to SSC ownership of various IT assets for networking, computer processing, audio visual, desktop software, and mobile telephones (cell phones, smart phones and satellite phones). This transfer reduced the number of IT assets required to be lifecycle-managed, but increased the number and type of services obtained from third parties that need to be managed. In fiscal year 2015–16, expenditures for all SSC assets and related services is estimated to be $4.8 million.

The audit interviews with IMTD revealed that there is currently no service level agreement (SLA) between SSC and the CNSC, and IMTD does not have mechanisms to record, track and monitor IT services provided by SSC that are used to meet business requirements.

Outsourcing services to SSC involves the transfer of responsibility from the CNSC to SSC. The management approach changes from management of the lifecycle of assets used to provide IT services to management of the outsourcing relationship. This includes the following aspects:

- A management strategy to determine the most appropriate combination of agreement terms and conditions in an SLA and to establish relationship management mechanisms.
- An organizational structure to build the in-house management oversight structure and mechanisms; IT Infrastructure – the supporting infrastructure to enable the monitoring and management of the various services outsourced and their providers.

Conclusion

A management structure for IT assets is in place, but the IT services management framework has yet to be defined for IT assets entrusted to the CNSC. IMTD indicated that an IT services management framework should be developed by SSC as it relates to their assets. IMTD is currently not maintaining its inventory. This approach is not in compliance with the Treasury Board policy.

2.1.2 Roles and responsibilities

The audit examined the extent to which roles and responsibilities are in place, approved and communicated to staff.

High level roles and responsibilities are outlined in the CNSC's Management of Information Technology Policy and the Information Technology Asset Management Directive. The policy includes the responsibilities of employees, managers and IMTD with respect to managing IT assets. The directive outlines specific employee and IMTD roles and responsibilities. The audit found that employees and IMTD staff understood their roles and responsibilities for managing and safeguarding CNSC IT assets.

Numerous CNSC IT assets have been transferred to SSC, and the CNSC is now receiving SSC services. For example, SSC is now responsible for providing the following services:

- Networking
- Cabling
- Computer processing capacity
- Voice

- Conferencing (i.e., video, audio, Web)

For services, the roles and responsibilities for employees and IMTD staff have yet to be developed, documented and implemented. Specifically, telecommunications services roles and responsibilities have not been defined and documented. As the roles and responsibilities with respect to service delivery are becoming an increasingly larger part of IMTD's activities, IMTD staff need to understand their changing role.

Segregation of duties

The Information Technology Asset Assignment and Tracking Procedures specify that the Asset Management Group consists of a Technical Support Centre (TSC) technician and the IT asset management officer. In the procedures, the roles are documented as being interchangeable with either person receiving assets, tagging assets, assigning assets, installing assets, updating asset records and identifying assets for disposal or destruction. Proper segregation of duties requires that the person with access to assets be segregated from those recording the asset information. This is to prevent assets from being removed and records altered without being detected.

The audit found that the IT asset management officer is responsible for recording and tracking all assets in the IT Asset Management System. However, the IT asset management officer also has access to IT assets in the storage rooms; the asset could be removed and records altered accordingly.

IMTD indicated that:

- every request is initialed and backed up by a ticket. Given the size of the organization, IMTD believes the responsibilities are properly defined and followed.
- restricted access to the storage rooms and assets are in place to minimize the risk.

We note that IMTD's comment does not address the segregation of duties. If the ticket was never created, or if the ticket was destroyed and the system altered, then the asset would appear as non-existent, and could be removed and not detected.

Restricting the access to the storage room only helps identify one of the three people who have access to assets in it (not the assets located in the offices). Removing the asset records could allow the asset to be removed and not detected as missing.

Conclusion

IMTD understands its roles and responsibilities for managing CNSC IT assets, but some incompatible roles exist. The management of IT services roles and responsibilities are not documented.

Recommendation 1

It is recommended that:

a. a directive and written procedures be developed to describe practices that will be used in managing the IT services
b. The roles and responsibilities be improved by:
    i) defining, documenting and communicating the roles and responsibilities with respect to management of IT services
    ii) segregating the Asset Management Group role into two separate functions:
        - asset recording
        - handling of inventory
c. IMTD develop and implement practices to be used until an SLA is entered into with SSC

Management response and action plan

Recommendation 1 a.
Management supports the recommendation.

Shared Services Canada – CNSC Interactions Standard for Telecommunications Services – e-Doc 4995600 – In order to address the recommendation, a new standard was created. Specifically, the new standard defines the demarcation of SSC and CNSC responsibilities for services provided by SSC along with service targets. This standard was written by the Information Management Division in consultation with the Telecommunications and Asset Management Officer. It was reviewed and approved by the SSC coordinator; the director, Information Technology Security and Services Division and the director general of IMTD. This new standard document was sent by email to the parties involved on June 22, 2016

September 21, 2016 update
Document includes reference to satellite telephones as a service.
Referencing procurement of its services (e.g., networking, applications and email), SSC has not provided adequate visibility to departments / agencies to demonstrate the cost and/or value of the services. As a result, they have not been included at this time.

Recommendation 1 b. i)
Management supports the recommendation.

Shared Services Canada – CNSC Interactions Standard for Telecommunications Services – e-Doc 4995600 – In order to address the recommendation, a new standard was created. Specifically, the new standard defines the roles and responsibilities of SSC and the CNSC. This new standard was written by the Information Management Division in consultation with the telecommunications and asset management officer. It was reviewed and approved by the Shared Services coordinator; the director, Information Technology Security and Services Division and the director general of IMTD. This new standard document was sent by email to the parties involved on June 22, 2016.

September 21, 2016 update
Document includes reference to satellite telephones as a service. Referencing procurement of its services (e.g., networking, applications and email), SSC has not provided adequate visibility to departments / agencies to demonstrate the cost and/or value of the services. As a result, they have not been included at this time.

Recommendation 1 b. ii)
Management supports the recommendation.

IT Asset Assignment & Tracking Procedures – e-Doc 3875336. In order to address the recommendation, the procedure was amended. Specifically, the revised document now segregates duties between the asset management officer and the IT asset TSC technician in relation to asset recording and inventory handling. This revised procedure was reviewed and updated by the telecommunications and asset management officer and approved by the director of ITSSD. This revised procedural document was sent to TSC on June 22, 2016.

Recommendation 1 c.
Management agrees with the recommendation.

Shared Services Canada – CNSC Interactions Standard for Telecommunications Services – e-Doc 4995600 – In order to address the recommendation, a new standard was created.
Specifically, the new standard defines the demarcation of SSC and CNSC responsibilities for services provided by SSC, along with service targets.

This standard was written by the Information Management Division in consultation with the telecommunications and asset management officer. It was reviewed and approved by the SSC coordinator; the director, Information Technology Security and Services Division and the director general of IMTD. This new standard document was sent by email to the parties involved on June 22, 2016.

September 21, 2016 update
Document includes reference to satellite telephones as a service.
Referencing procurement of its services (e.g., networking, applications and email), SSC has not provided adequate visibility to departments / agencies to demonstrate the cost and/or value of the services. As a result, they have not been included at this time.

Completion date:

1 a.	Completed[1]
1 b. i)	Completed[1]
1 b. ii)	Completed[1]
1 c.	Completed[1]

[1] Management indicated that the MAP with respect to specific recommendations has been "completed". The OAE team has not validated management's assertions. As part of the follow-up of the MAPs, the OAE team will review management's assertions. If the team is satisfied with management's assertions, OAE will recommend that the Departmental Audit Committee approve the closure of the completed action plan.

2.1.3 Policy development

IT asset policy

The audit expected to find approved policies in place and communicated to staff for the management of IT assets both owned and entrusted to the CNSC.

The audit found that:

- the approved policy-related documents use a version control footer (containing version/e-Doc, effective date, approval date and next revision date) to track changes. In several instances, the version control footer was not present, incomplete or inaccurate. For example, the version control footer was missing in both the Management of Information Technology Policy and Procurement of Information Technology Hardware and Software Standard.

- The draft Corporate Services Branch (CSB) Policy Management Guide does not indicate the following:
  - what information is required in the various policy documents
  - how changes to policy documents are to be completed
  - what process is to be followed for reviewing the documents before publication

The audit found that a CSB policy review spreadsheet used to monitor revisions relies on e-Access to track versions. The audit noted that numerous changes had been made to policy documents: Management of Information Technology Policy, Information Technology Asset Management Directive, Mobile Communication Device Directive, Capital Asset Directive, and Procurement of Information Technology Hardware and Software Standard. However, there is no evidence to indicate what changes were made and when, whether they were approved (and by whom), or whether they were communicated to staff. Furthermore, IMTD indicated that:

- the CSB policy review spreadsheet includes planned review timelines; the audit found that the review process was not mentioned in the draft CSB Policy Management Guide.
- the Mobile Communications Device Directive and Information Technology Asset Management Directive were both updated in 2015. Some reviews were waiting until a Shared Services Canada impact could be integrated.

The audit found that there was no formal process in place:

- to regularly monitor published related IT asset policies, directives, standards, guidelines and procedures, to ensure that they are being periodically reviewed and updated. We note that in 2012, several IT asset categories were transferred to SSC, but the associated policy/directive related documents were not revised. For example, the IT asset definition as set out in the Information Technology Asset Management Directive has not been updated. This impacts the accuracy of the directive and associated procedures causing confusion on what assets are under the CNSC's management responsibility. Similarly the Mobile Communications Devices Directive has not been updated to reflect that cellular phones and smart phones are now part of the SSC telecommunications voice and data services, leaving only laptops within the definition of mobile devices.

- To ensure that only approved IT asset-related documents are posted on BORIS, IMTD indicated that:
    - only certain people have rights to publish content to BORIS, and these people each have restricted areas they can publish to. HTML versions of policies are being removed and replaced with links to the e-Docs, which should alleviate the chance of the HTML not matching with the up-to-date policy.
    - since a policy template that is used (which would cover content, form, and structure), a policy writing guide is not included, but language style should be adapted from previous CNSC policies.

The audit found that:

- a CSB policy framework document is in place; however, it should be strengthened by including the rationale and principles on which the CNSC policy instruments will be based.
- A draft CSB policy management guide is in place; it needs to be reviewed in order to ensure that it is consistent with CNSC's policy suite renewal structure and should then be approved, communicated to all stakeholders, and implemented.
- Some IT asset-related procedures are not being followed. For example, the Information Technology Asset Management Directive requires employees on long-term leave to return assigned or borrowed assets to IMTD. As part of our inventory count, the audit team found 16 employees on long-term leave had not returned their assets to IMTD. Also, non-readable asset tags should be replaced. Our inventory count found 21 instances of IronKeys in which the asset tag was obliterated and not replaced.

Telecommunications policy

A telecommunications policy document for managing acquired services is not in place. IMTD indicated that they believe they have no role in managing IT assets provided by SSC given that SSC assumed this responsibility when the assets were transferred.

The information technology trend is for departments to increasingly procure services rather than own the assets used to provide a service. Managing the procurement of outsourcing services from third parties requires a different management framework. It is clear in the Treasury Board's Policy Framework for the Management of Assets and Acquired Services that departments are required to implement management activities "to provide value for money and demonstrate sound stewardship in program delivery".

Conclusion

The audit found that draft policy suite-related documents for the management of IT assets are generally in place (policies, directives, procedures and guides). These documents need to be: (a) reviewed to ensure that they are up to date; (b) approved; (c) communicated to the staff; and (d) implemented.

Recommendation 2

It is recommended that:

a. the draft policy suite-related documents, including procedures related to the Information Technology Asset Management Directive be updated, approved and communicated to all stakeholders
b. procedures relating to service procurement be developed, approved, and communicated

Management response and action plan

Recommendation 2 a.

Management agrees with the recommendation.

Asset Management Directive: e-Doc 3840611

IMTD Process – IT Asset Procurement: e-Doc 4999678

IMTD Process – Wireless Device Requests: e-Doc 4984301

In order to address the recommendation, the Asset Management Directive was amended and asset procurement and management processes were created. Specifically, the revised directive's footer was properly updated to include accurate directive update and revision dates. The asset procurement and wireless devices processes were created to clarify roles and responsibilities.

The updated directive was reviewed and approved by the chief information officer, and the processes were reviewed and approved by the director, ITSSD. The contents of these documents have been communicated to TSC staff as appropriate.

Recommendation 2 b.

Management supports the recommendation.

IMTD Process – Wireless Device Requests – e-Doc 4984301 – In order to address the recommendation, a new process was created. Specifically, it describes the process to follow to obtain telecommunications services from SSC.

The process was created by the Information Management Division in consultation with the telecommunications and asset management officer. It was reviewed and approved by the SSC coordinator and director, Information Technology Security and Services Division. This new process document was sent by email to the parties involved on June 22, 2016.

July 13, 2016 update – Document has been updated and renamed to Shared Services Canada (SSC) Service Procurement Procedures and includes documented procedures for videoconference and landline services.

September 21, 2016 update – CNSC Interactions Standard for Telecommunications Services – E-doc 4995600

Document includes reference to satellite telephones as a service.

Referencing procurement of its services (e.g., networking, applications and email), SSC has not provided adequate visibility to departments / agencies to demonstrate the cost and/or value of the services. As a result, they have not been included at this time.

Completion date:

2 a. Completed[1]
2 b. Completed[1]

2.2 Line of enquiry 2 – Lifecycle management practices are in place for IT assets

This line of enquiry was to assess the lifecycle practices over the processes in place for planning the acquisition, replacement and disposal of CNSC owned assets.

2.2.1 Planning

The CNSC Procurement of Information Technology Hardware and Software Standard identifies a standard hardware and software configuration for employees based on their role at the CNSC. Exceptions only occur when the results of an ergonomic assessment require non-standard equipment to be installed.

The CNSC maintains a storage area that retains the reserve supply of IT assets. Reserves are based on a three year IT Asset Lifecycle Plan which outlines annual desktop and laptop computer replacements. Computers are purchased when they do not meet the minimum standard computer configuration available through the

Government of Canada’s National Master Standing Offer for computer equipment.

The audit found that the IT Asset Lifecycle Plan for computers is four years, which is reasonable based on Treasury Board *Accounting Standard 3.1-Capital Assets* (this standard identifies the capitalization period for computer hardware to be 3 to 5 years). Also, the process used for identifying computer replacement provides a cost effective mechanism for the regular replacement of computers.

For desktop software, SSC is responsible for licensing all standard desktop software (operating system and office productivity suite) while the CSNC is responsible for non-standard software licensing. New non-standard software is only purchased if the need for software is justified by the directorate for an identified business requirement and meets IMTD financial and technical reviews.

Replacements and acquisitions

IMTD is the only directorate responsible for procuring IT assets. Standard desktop hardware is procured quarterly (or when demand dictates) from the National Master Standing Offer using the Asset Lifecycle Plan. IMTD’s annual operational budget includes the lifecycle hardware assets replacements in the plan.

Non-standard desktop hardware is procured, if items are not available in the storage room, and directorates provide proper justification and funds. IMTD completes a financial and technical review before initiating the procurement.

As described earlier, IMTD is only responsible for the procurement and upgrade of non-standard desktop software, as standard software (operating system and office productivity suite) is provided by SSC.

The audit found the replacement and acquisition process and controls are effective in replacing standard assets at the end of their useful life and non-standard assets to meet business requirements.

IMTD maintains an inventory of non-standard software that identifies which desktops they are installed on. When new versions of the non-standard software are identified by IMTD, they must pass a technical review before new licences are procured and software is installed. IMTD incurs the expense for upgrades to non-standard software.

The audit found the acquisition and upgrading of non-standard software to be a cost-effective method for meeting the business requirements.

Planning for disposals

Assets are identified as surplus based on criteria specified in the Information Technology Asset Assignment and Tracking Procedures. The following replacement factors are used:

- Asset age – includes computer equipment that has reached four years of age
- Relevancy – assets that no longer have any business use
- Performance – no longer meets technological requirements (i.e. technology obsolete)
- Other priorities – surplus to CNSC operations
- Defective and beyond economical repair
- Technical upgrade

The audit found the criteria effective in obtaining the maximum benefit from IT assets.

Conclusion

Effective processes are in place for planning with respect to the acquisition, replacement and disposal of CNSC IT assets.

2.2.2 Process and procedures

The audit expected to find a formal documented process in place for planning the acquisition, replacement and disposal of CNSC IT assets.

Replacements and acquisitions

The CNSC has processes in place for planning the acquisition of hardware and software, but the acquisition procedure is not documented. All procurement and purchasing is centralized in IMTD and once procured, assets are tagged and entered into the asset management system and tracked by an IT Asset Management Agreement until disposal criteria is met.

IMTD indicated that acquisition procedures are not part of the document. The OAE included the acquisition procedures as they were included as part of the asset lifecycle in the Audit Planning Report tabled at the Departmental Audit Committee in July 2015.

Disposals

IT assets are identified as surplus based on the IT asset lifecycle criteria or other specific criteria specified in the Information Technology Asset Assignment and Tracking Procedures.

The procedures are not clear on what items can be sent to the Computers for School (CFS) program, which IT assets require alternate means of destruction, and how destruction must be accomplished.

IMTD indicated that the list of items that can be sent to CFS is provided by Industry Canada. Items that are not on the list are still being picked up by Industry Canada, but they are delivered to a recycling facility. The audit found that the list was not included or referenced in the procedures.

Once an IT asset is identified for disposal or destruction, the IT asset disposition officer should control all surplus assets until disposal to the CFS program or destruction. Instead, the audit found that the procedures do not require the IT asset disposition officer to sign an IT Asset Assignment Agreement form to take custody and control of the asset. The officer must acknowledge receipt of the IT asset and maintain custody of the assets, otherwise it is difficult to hold the officer accountable for these assets.

IMTD indicated that the IT asset disposition officer (as stated in the procedures) has a copy of the final report of assets to be disposed of and is present at the time of disposition to verify that each asset shows up on the report prior to leaving the CNSC. After verification of all assets, the IT asset disposition officer signs the report. The Industry Canada employee picking up the equipment follows the same process.

Once completed, the report is provided to the asset management officer, who then updates the asset tracking system.

The audit identified that the list is not prepared by the IT asset disposition officer. The list is prepared by the IT asset management officer who records all changes to assets. If the IT asset disposition officer creates their own list from the assets they sign for and compare to what is in the business record, they could confirm that the assets for disposal have all been properly identified and removed from the asset management spreadsheet. The Information Technology Asset Assignment and Tracking Procedures require that the CFS assets and assets scheduled for disposal be housed in a locked, caged area until they are removed for disposition. However, the procedures do not require the IT asset disposition officer to control all access to the caged area. Instead, the audit found that the TSC technician was placing the assets in the caged area and the gate was not being locked. Due to the design of the storage room, the IT asset disposition officer must access the regular asset storage area before reaching the disposal cage. Regular inventory is at risk if the IT asset disposition officer accesses the storage room. Separate access to the inventory storage area and the asset disposal area are required.

IMTD indicated that it has limited storage space. The OAE found that IMTD’s comments do not address separate access to regular storage and surplus assets.Some surplus assets may contain sensitive CNSC information. IMTD has instituted a process to wipe desktop and laptop computers' hard drives before disposal. The TSC technician uses RCMP-approved software to clean all data before the IT asset is ready for disposition. Although hardware data wiping is being performed on computers on a regular basis, it has not been included the Information Technology Asset Assignment and Tracking Procedures, and there are no requirements for wiping other IT assets.

Several improvements must be made to the procedures and storage room design to properly control disposition of IT assets.

The audit team found that the process for transmitting IT assets to CFS was in place, documented and properly controlled.

Conclusion

Processes are in place for the acquisition, replacement, and disposal of IT assets, but procedures are not documented for acquisition of IT assets. Improvements are required to procedures before the disposal of IT assets can be properly controlled.

Recommendation 3

It is recommended that lifecycle procedures and controls be improved by:

a. developing, approving, and communicating the procedure for the acquisition of hardware and software
b. revising current procedures to describe:
    i) items for disposal and their method of disposal
    ii) items for the Computers for School program and procedures for removing sensitive information from media
c. documenting the process for IT disposition including the controls over tracking and safeguarding of surplus assets

Management response and action plan

Recommendation 3 a.

Management agrees with the recommendation.

IMTD Process – IT Asset Procurement – e-Doc 4999678 – In order to address the recommendation, a new process document was created. Specifically, it outlines the procedures to be followed for the procurement of hardware and software. This process was prepared by the Information Management Division in consultation with the various groups involved in the procurement process. It was approved by the director, Information Technology Security and Services Division.

Recommendations 3 b. i) ii)

Management agrees with the recommendation.

IT Asset Assignment & Tracking Procedures – e-Doc 3875336. Item 4.5, Step 3. In order to address the recommendation, the procedures document was reviewed and amended. Specifically, it describes the method of disposal of equipment for the Computers for School program and the procedures for removing sensitive data before disposal.

This revised procedure document was reviewed by the telecommunications and asset management officer and approved by the director, Information Technology

Security and Services Division. This revised procedures document was communicated to TSC staff on June 22, 2016.

Recommendation 3 c.

Management agrees with this recommendation.

IT Asset Assignment & Tracking Procedures e-Doc 3875336. Item 4.17 - Asset Disposal. In order to address the recommendation, the procedures document was reviewed and amended. Specifically, it demonstrates the segregation of duties of all parties involved in the disposition of equipment including the controls over tracking and safeguarding of surplus assets.

This revised procedures document was reviewed and amended by the telecommunications and asset management officer and approved by the director, Information Technology Security and Services Division. This revised procedures document was communicated to the TSC on June 22, 2016.

Completion date:

3 a. Completed[1]

3 b. Completed[1]

3 c. Completed[1]

2.2.3 Audit criteria 2.3

IMTD complies with the CNSC and Treasury Board policies for acquisition and disposal of IT assets.

Planning and acquisition

The Treasury Board *Policy on Investment Planning – Assets and Acquired Services* requires that investment plans be developed to allocate and reallocate resources to new and existing assets and acquired services for program delivery. IMTD prepared the three-year *Departmental Information Technology Plan 2015–18*, which supports planned expenditures. In the *Policy on Management of Materiel* requires that assets be safeguarded and management information systems be in place to ensure records are accurate and reliable. The audit found that IMTD complies with these relevant Treasury Board policies.

Disposal

The Treasury Board *Directive on Disposal of Surplus Materiel* requires that surplus IT assets be offered first to the Industry Canada Computers for Schools (CFS) program. The CNSC is in compliance with the TB Directive as IT assets are being properly identified for the CFS program.

Conclusion

IMTD processes comply with CNSC and Treasury Boards policies with respect to acquisition and disposal of IT assets.

2.2.4 Audit criteria 2.4

IMTD has developed and implemented hardware and software guidance for procurement.

IMTD has developed a procurement of IT hardware and software standard to assist users in requesting IT assets that connect to the CNSC network. The document clearly identifies the IT assets covered and the process to be followed; however, the document needs to be updated to remove references to assets transferred to SSC.

Hardware and software standards are based on the employee’s role at the CNSC, not on what the specific employee desires. Employees are provided with a standard IT configuration based on their position. If an ergonomic study recommends non-standard equipment, the items are usually approved by IMTD for procurement.

For any other non-standard equipment, the employee’s Director must justify the request and have the budget to cover the expenditure before being approved by IMTD for procurement.

All approved IT asset requests are sent to the TSC Help Desk and are controlled by a ticket number until purchased or the request is denied. IMTD has implemented a procurement process that requires several reviews to be completed before being approved for procurement:

- SSC review
- IM/IT policy review
- IT security review
- Product assessment (software) review
- Product assessment (hardware) review

Only once the reviews are completed will the items be sent to the IT procurement officer to perform the required procurement activities.

IMTD follows this process which has been documented by a high level process flowchart.

The audit found that the procurement standard is being followed by IMTD.

Conclusion

IMTD has implemented an effective procurement standard to control IT asset procurement.

2.2.5 Audit criteria 2.5

The CNSC mitigates the risk of employees benefiting from the purchase and disposal of IT assets.

The procurement process is properly segregated from the asset management process; however, weaknesses found in the asset management roles and responsibilities must be addressed.

When certain employees have the ability to record the movement of IT assets from inventory to disposal and are able to access assets in storage, there is an increased risk that assets of value could be removed from inventory without being detected. The IT asset management officer should not have any access to physical inventory (in storage, CFS or assets slated for destruction).

IMTD indicated that due to the size of the organization and the amount of staff it is difficult to segregate the duties. It should be noted that every IT asset activity (e.g., moves, adds or removals of equipment) are backed up by a ticket issued by the TSC with director approval.

The audit team noted that the Asset Management Group consists of two employees who agree to have their roles and responsibilities separated into the two required roles. The procedures could be modified to reflect these two separate roles.

Conclusion

Improvements are required to roles and responsibilities and to restricting access to valuable assets (and those slated for destruction). This issue is addressed in recommendation 2 b.

2.3 Line of enquiry 3 – Processes and systems exist for assets owned by the CNSC

This line of enquiry assesses the processes and systems that are in place to record, track, monitor, and safeguard the IT assets owned by the CNSC.

2.3.1 Audit criteria 3.1.

An IT asset tracking system is in place for IT assets, and access is restricted to authorized staff.

Asset tagging

A process exists for identifying CNSC IT assets from the time of procurement until disposition. The audit found that some assets are not being tagged (i.e., e-tokens). This makes it difficult to identify CNSC assets.

For IronKeys, a unique asset tag type is being used: the asset number starts with a “U”. The audit found these tags are not as durable as the other asset tags, as 21 out of 708 items were found with obliterated tags during the inventory count. IMTD indicated that these tags are no longer used. New IronKeys will be tagged with the latest asset tags.

The asset tagging process is not accurately documented in the Information Technology Asset Assignment and Tracking Procedures. The procedure indicates that anyone in the Asset Management Group can tag assets and enter it into the asset tracking system. In practice, the sole TSC technician controls all movement of assets in and out of inventory storage. The other member of the Asset Management Group, the IT Asset management officer is the only person updating the asset tracking system. These roles need to be clarified in the procedure.

When assets were transferred to SSC, the CNSC asset tags were not removed from the asset or from the asset management system. This makes it more difficult to determine whether the asset belongs to the CNSC or SSC. For example, network switches and hubs were transferred to SSC, but the audit found several switches and hubs located in CNSC offices with only CNSC asset tags. When the assets were transferred to SSC, the process did not require the CNSC asset tags to be removed or marked in a way to indicate the asset had been transferred. In fact, many assets that were transferred to SSC remain in the CNSC inventory records.

Also, when older USB keys were replaced with IronKeys, the older USB keys were not collected and destroyed (making these USB keys vulnerable to sensitive information exposure if not properly wiped). The audit inventory count found 33 employees with older USB keys still marked with CNSC asset tags; however, these asset tags were not in the asset management system, increasing confusion as to whether or not they were CNSC assets. Orphaned assets should be tracked until they are received for destruction and/or replaced with an IronKey.

Improvements are required to the asset tagging process and roles and responsibilities. The Information Technology Asset Assignment and Tracking Procedures must be clarified and followed. Older USB assets should be recalled and replaced with compliant IronKeys.

Recommendation 4

It is recommended that the asset tagging procedures and controls be improved by:

a. placing an asset tag on all CNSC assets
b. having the TSC technician tag all newly acquired assets before placing them in the inventory
c. removing or obliterating asset tags on assets transferred to SSC
d. procuring asset tags that can withstand wear.
e. collecting assets considered obsolete and ensuring disposition takes place

Management response and action plan

Recommendation 4 a.

Management agrees with the recommendation.

All CNSC assets must have an asset tag, space permitting. Certain assets such as e-tokens do not permit an asset tag given the lack of physical space. In such circumstances, the serial numbers are used to track the devices.

Recommendation 4 b.

Management agrees with the recommendation.

IT Asset Assignment & Tracking Procedures – e-Doc 3875336. Item 4.10 Receiving and Tagging Assets. In order to address the recommendation, the procedures document was reviewed and amended. Specifically, it demonstrates the segregation of duties between the IT asset management officer and the IT asset TSC technician for the receiving and tagging of new equipment.

This revised procedures document was reviewed and amended by the telecommunications and asset management officer and approved by the director, Information Technology Security and Services Division. Additionally, this revised procedures document was sent to all parties involved. This revised procedures document was sent to ITSSD parties on June 22, 2016.

Recommendation 4 c.

Management agrees with this recommendation.

CNSC tags will be removed from SSC IT assets by June 2016.

Recommendation 4 d.

Management agrees with this recommendation.

In 2012, inferior quality tags were purchased which resulted in premature wear. IMTD now uses more robust asset tags that can withstand wear.

Recommendation 4 e.

Management agrees with this recommendation.

In order to address the recommendation, an email was sent to users for the recall of the old USB keys. All but two USB keys have been returned. Follow-up emails have been sent with cc to Management. Disposal for destruction is done on a yearly basis. USB keys will be sent on the next destruction shipment at the end of the fiscal year.

October 4 2016 – Update

IMTD confirmed with the employee that no personal or sensitive information was saved on the USB keys. The two outstanding USB keys have been returned. As a result, no further action is required.

Completion date:

4 a. Completed[1]

4 b. Completed[1]

4 c. Completed[1]

4 d. Completed[1]

4 e. Completed[1]

System for tracking IT assets

The audit found that two systems are being used to record IT asset information. The main asset management system consists of two spreadsheets – one is used for tracking hardware and the other software assets. Staff consider these spreadsheets the official IMTD IT asset management records. IMTD indicated that the spreadsheet is leveraged to produce various reports on IT assets.

The audit found that IMTD uses a second asset management system. A custom off the shelf (COTS) system that was implemented in response to audit findings included in the Audit of IT Asset Management Report (July 10, 2012). Audit findings indicated that asset management staff found that the COTS system is not useful, as they are unable to produce the required reports needed to manage inventory.

At this time, both the spreadsheet and other system are being updated in parallel with the same input, but there is no mechanism in place to ensure both systems contain the same IT assets.

IMTD relies upon the hardware and software spreadsheets as the official asset management records for managing IT assets. Currently, the COTS system is only being used to assist in locating assets, as it has an audit trail which shows the movement of assets. The spreadsheet does not currently contain an audit trail of transaction history. IMTD indicated that the spreadsheet is being modified to include an audit trail mechanism and is testing the changes at this time.

Duplicating entry of transactions into two systems is inefficient and uneconomical. If the COTS system is to be the official IT asset management system, IMTD needs to investigate why the IT asset management functionality has not been fully implemented.

Asset record management

The CNSC asset spreadsheet contains a mixture of SSC- and CNSC-owned assets. The audit team found the following SSC-owned asset types are still in the spreadsheet:

- network switches and hubs
- audit visual communication devices
- cell phones, smart phones and satellite phones

Only CNSC-owned assets should be included on the CNSC hardware spreadsheet; all other assets should be removed from the spreadsheet and asset tags obliterated so that CNSC assets are easily recognizable. Removing SSC assets will decrease the current confusion about which assets the CSNC owns.

Access to inventory records

Access to the hardware and software asset management system records was found to be appropriately restricted to the IT asset management officer.

The spreadsheet for hardware and software is only updated by the IT asset management officer who secures the files with a password. The TSC technician is the only other person using the inventory information and has read-only access.

Conclusion

An asset tracking system is in place and access is properly controlled. However, improvements are required:

- in the process for tagging assets
- eliminating a duplicate asset tracking system
- removing SSC assets from the hardware spreadsheet used for inventory tracking

Recommendation 5

It is recommended that:

a. a study should be conducted of the COTS system to determine which functionality is missing or not functioning, as required, and corrective action should be taken
b. the process and associated procedures be improved to accurately reflect which assets are under CNSC management by clearly marking items with asset tags and accurately reflecting the asset in the asset management system

Management response and action plan

Recommendation 5 a.

Management agrees with the recommendation.

October 4 – Update

IMTD has completed the analysis of the COTS system and the requirements have been incorporated into the IMTD service management tool assessment. Procurement is expected to occur during fiscal year 2017–18.

Recommendation 5 b.

Management agrees with the recommendation.

IT Asset Assignment & Tracking Procedures – e-Doc 3875336, Appendix A – Tagged and Excluded Items List. In order to address the recommendation, the procedures document was amended. Specifically, appendix A shows the CNSC items that are to be tagged and items that are tracked by serial numbers.

This revised procedures document was reviewed and amended by the telecommunications and asset management officer and approved by the director, Information Technology Security and Services Division. This revised procedures document was sent to the TSC on June 22, 2016.

Completion date:

5 a. Completed[1]

5 b. Completed[1]

2.3.2 Audit criteria 3.2

The audit expected to find that the IT assets records and information were complete and accurate and periodically verified to ensure IT assets had not gone missing.

Verification of hardware asset records

The Information Technology Asset Assignment and Tracking Procedures require that an annual inventory of all assets be undertaken. In 2014, an asset inventory was conducted. However, this inventory only included the desktop hardware as part of the desktop modernization project and count of laptops, which represents approximately 75 percent of the assets. Appendix D identifies the remaining approximate 25 percent of IT assets which should have been inventoried. Therefore, in 2014, the inventory procedure was not followed during the conduct of the inventory of IT assets.

It should be noted that the inventory count conducted by audit confirmed that all desktop computers and laptops were located.

Verification of software asset records

An annual inventory of software assets is not being conducted to verify the accuracy of the software inventory information. IMTD indicated that they do not have the tools to scan computers in order to identify which software and associated licence code is loaded on a computer. As a result, they are unable to verify the accuracy of the software installed against software licences owned by the CNSC.

IMTD indicated that it currently has a tool – Microsoft System Center Configuration Manager (SCCM) – which confirms about 80 percent of the software inventory. The only issue is Adobe licences because of the various software packages that can be found in Adobe Suites.

OAE does not agree that SCCM is an appropriate software verification tool and will result in the risk of the CNSC installing licences it has not purchased.

IMTD stated that they investigated using the existing system manager software tool to identify the applications and licence information. The existing tool does not identify software by specific licence. Therefore, information cannot be compared to the software licensing spreadsheet. For example, some software is delivered as a suite that includes several individual applications for one licence. However, the tool shows them individually and not as the suite.

IMTD believes that procuring a specialized software licensing management tool to measure licence use would not be cost effective. The CNSC relies only on complete and accurate processing software requests to update the software inventory spreadsheet. IMTD does not have a mechanism for assessing the accuracy of the software licence spreadsheet. By not comparing the application licences installed against licences owned, the CNSC increases its risk of having illegal software installed on its computers.

Verification of telecommunications assets

For telecommunications equipment owned by SSC, but assigned to CNSC employees, the CNSC does not maintain a list of active telecommunication devices (i.e., landline phones, cell phones, smart phones and satellite phones). Some the information remains in the IT hardware asset spreadsheet on smart phones, cell phones, and satellite phones, but it is not being maintained as SSC has taken over providing this service.

IMTD does not want to assume responsibility for maintaining such lists, as SSC is responsible for managing the physical devices. However, the CNSC uses the services provided by these assets and has not implemented any mechanisms to determine if the required services being obtained meet their requirements and are consistent with those agreed to. Telecommunications services such as landline phones, cell phones, smart phones, and satellite phones need to be periodically verified to ensure the CNSC is being charged for the correct number of active lines.

For example, the inventory count audit attempted to locate satellite phones which were included in the IT asset inventory. Satellite phones play an important operational role in the event of a nuclear incident. Not having the correct telephone number and location could result in delays in responding to incidents.

The audit compared the CNSC asset inventory list of satellite phones to the SSC list and found the following:

- SSC had 17 satellite phones listed at SSC, while IMTD only had 15 listed. The discrepancies were related to a roof top unit not accounted for at headquarters, and a fixed phone located at Darlington.
- Several CNSC satellite telephone numbers were inaccurate. The audit team was advised that SSC had changed the numbers, but IMTD was not made aware of the changes. The CNSC asset tags were found on some phones, but generally serial numbers were used as asset identifiers.
- Two CNSC satellite phones were not identified as being located in source recovery vehicles.

Audit verification of inventory

The audit team conducted a complete inventory count of IT assets to verify the accuracy of asset management records as at May 4, 2015. While 9,170 items were identified in the list provided by IMTD on May 4, 2015, the OAE verified 9,328 items during the inventory count. The 158 difference represents assets that were verified that were not on IMTD's list.

The audit team found the following:

1. Of the total items inventoried, 4 percent (389/9,328) of the items could not be located. The reasons identified for the discrepancies were as follows:
    - Assets could not be found
    - Assets could not be found, and employee no longer at the CNSC
    - Asset could not be found, but was replaced with another asset
    - Asset was lost or broken and replaced
    - Asset could not be located, as employee is on long-term leave
2. For assets found, 7.5 percent (696/9328) of the asset inventory information contained errors. The reasons for the errors included the following:
    - Asset locations were incorrect
    - Assets were found, but were not included on the inventory list
    - Assets found, but employee no longer at the CNSC
    - Assets found were not tagged
    - Asset tags were unreadable
    - Assets belonged to an employee on long-term leave, but were not retained under CNSC control.

3. The audit found that all material computer assets were located; items not found were of a lower dollar value. From a risk perspective, the audit team was concerned and recommended that IT assets which could contain sensitive business data such as hard drives, smart phones, and USB devices be located. During the audit team’s review, the following assets were not found:

Table 1 – IT assets not verified by audit

Device type	Number not found
External hard drives	8
Tablets	3
USB keys	52
Wireless devices	80

Table 1 identifies missing assets as at September 9, 2015. IMTD had not provided evidence to the OAE that the items had been located.

If these assets were found and not properly protected, sensitive CNSC information might be compromised. IMTD should investigate whether any of the items not found likely contained sensitive information and whether security controls were in place to prevent access to the information.

TSC loaner pool verification

The TSC loaner pool consists of several assets assigned to the pool for short-term borrowing. Assets loan requests by employees are made to TSC help desk agents, who record the request into the help desk ticketing system. The audit team found that asset tag information is not always entered into the ticketing system or on the IT Short-Term Loan Agreement form. This makes it difficult to identify which asset(s) were on loan.

The audit team was advised that a TSC technician performs a periodic inventory of the TSC loaner pool, but procedures on loan pool inventory-taking are not included in the Information Technology Asset Assignment and Tracking Procedures to ensure all assets in the pool have a properly signed agreement or are located in the locked cabinets. Discussions with a TSC Technician revealed that only laptop computers were being counted and not the entire pool contents.

All loaner pool assets should have a corresponding signed IT Short-Term Loan form or be present in the secure container. During the inventory count, several items assigned to the TSC loaner pool could not be located. A review of the report from the ticketing system helped the audit team to reconcile some of the differences.

The loaner pool included 84 items which represented the combined IT assets at Slater and Telesat. The audit team's inventory count found the following with respect to the loaner pool:

- 26 percent (22/84) missing items (not laptops)
- 1 percent (1/84) description inaccurate
- 1 percent (1/84) item found but not recorded in loan pool inventory

With the high movement of items in the loaner pool, IMTD must conduct a complete inventory on the loaner pool assets more frequently than once a year to detect missing assets – especially those that could contain sensitive information.

Conclusion

IT hardware asset records are not always accurately reflected in the IT asset management system:

- Material computer assets records are accurate.
- Other IT hardware asset records are not accurate, as the verification process does not ensure that they are being counted.

IT software asset records are not being verified. The completeness and accuracy cannot be determined.

Recommendation 6

It is recommended that:

a. the accuracy of assets be improved by
    i) having all assets verified during the annual verification and the loaner pool inventories verified on a more frequent basis
    ii) implementing a software licencing verification tool
    iii) periodically obtaining telecommunications asset information from SSC and verifying it against CNSC-collected information
b. steps be taken to locate assets missing during the inventory count that could contain sensitive business information

Management response and action plan

Recommendation 6 a. i)

Management agrees with the recommendation.

IMTD has implemented a mandatory monthly verification of the loaner pool for all devices.

July 13 2016 Update – IMTD conducts an annual verification of all CNSC IT assets on an annual basis.

Recommendation 6 a. ii)

Management agrees with the recommendation.

SSC has recently released a Request for Information (RFI) in order to obtain a government-wide solution for IT asset management (including a licencing software verification tool). Once procured by SSC, the CNSC will implement the tool.

October 13 2016 Update

As an interim solution to SSC's enterprise tool, IMTD will implement the licence compliance feature on the SCCM tool, which will track the number of software licences in the Production and Lab environment.

Recommendation 6 a. iii)

Management supports the recommendation.

IMTD Process – Wireless Device Requests – e-Doc 4984301 – In order to address the recommendation, a new process document was created. Specifically, the new standard includes the process to follow when ordering wireless services from SSC. Effective April 1 2016, IMTD began receiving and validating usage reports from SSC, and verifies them against CNSC-collected information.

This process was written by the Information Management Division in consultation with the telecommunications and asset management officer. It was reviewed and approved by the SSC coordinator and approved by the director, Information Technology Security and Services Division. This new process document was sent by email to the parties involved on June 22.

July 13 2016 Update – Document has been updated and renamed to Shared Services Canada (SSC) Service Procurement Procedures and includes documented procedures for videoconference and landline services.

Recommendation 6 b.

Management agrees with the recommendation.

All assets identified in the audit were located and have been added to the inventory.

Completion date:

6 a. i)	Completed[1]
6 a. ii)	Q4 2016-17
6 a. iii)	Completed[1]
6 b.	Completed[1]

2.3.3 Audit criteria 3.3

IT asset inventories are properly safeguarded when not in service, or scheduled for disposal.

Hardware assets

New hardware assets are received by the Commissionaires, who inspect the condition of the asset(s) for any damage before accepting them. The Facilities Group advises the TSC technician, who places the item(s) in the storage area. Assets received are taken to either the Slater TSC technician's room or the basement storage area for tagging. Access to the TSC technician's room is restricted to either the TSC technician or IT asset management officer, and the doors remain locked at all times. Access is controlled by a badge reader and security alarm system, and monitored by closed circuit television (CCTV).

Similarly, at Telesat, TSC maintains a separate locked room to store assets awaiting installation or new assets received and tagged. At Telesat, access is restricted to TSC technicians responsible for the installation of hardware. Access is controlled by a badge reader and security alarm system, and monitored by CCTV.

The TSC loaner pool is located at Slater in lockable cabinets. The cabinets are located in an open office where several employees work. Although the cabinets are left open during working hours, there is always a TSC help desk agent present monitoring who accesses the storage cabinet. At the end of the day the cabinets are locked.

Software media

All software media purchased is entered into the software asset management spreadsheet and placed in a lockable software storage cabinet (CD, stored on an application server, purchased as a downloadable media). The software cabinet is locked and access to the application server is controlled. When a TSC technician receives a software request, the software is removed from the locked cabinet by the IT asset management officer or downloaded from the application server by the TSC technician for installation purposes. CDs are returned to the locked cabinet.

The audit found that safeguarding controls over hardware and software storage were adequate and were being followed.

Conclusion

IT assets are properly safeguarded when not in service or scheduled for destruction.

2.3.4 Audit criteria 3.4

IT assets identified for disposal follow the TB Directive on Disposal of Surplus Materiel and are removed from the tracking system once they leave the CNSC.

For assets meeting the disposal criteria for the CFS program, the temporary status is changed to “Marked for CFS”. Action is then taken to replace the asset, and the TSC technician wipes the computer’s hard drive using the RCMP-certified software “KillDisk”. Once wiped, the computer is moved to the CFS caged area in the Slater basement storage area. When sufficient assets are accumulated, shipping arrangements are made to send the items to the CFS program. Once shipped and confirmation of receipt is obtained, the status is changed to “sent to CFS”. The record is then moved to the assets disposed asset tab for audit trail purposes.

The process with respect to identifying assets for disposal is consistent with the TB Directive on Disposal of Surplus Materiel and properly removed from the active assets inventory.

Conclusion

IT assets identified for disposal follow the TB disposal directive requirements and are properly removed from the tracking system.

2.3.5 Audit criteria 3.5

Mechanisms should be in place for ensuring sufficient licences exist for the number of installed applications.

The audit found that the IT asset management officer updates the spreadsheet software for assets procured, installed, or uninstalled based on TSC work requests. As the numbers of installed software requests are processed, the remaining licences are calculated. However, there is no method in place to periodically reconcile the inventory of software licences installed against those owned and shown in the asset management system.

Conclusion

There is no assurance that software installed does not exceed the licences owned by the CNSC. See discussion in section 2.3.2.

3 Overall conclusion

There is an established management framework in place, designed to promote general oversight, accountability, risk management and control over IT assets. However, there are a number or areas in which further enhancements are required to mechanisms, practices and controls. In addition, the management framework over telecommunication services procured from SSC needs to be developed and implemented.

The audit found that material IT hardware asset records were accurate and reliable, but lower dollar items had a higher degree of inaccuracy. For software assets, the accuracy and reliability of the information could not be assessed, as there was no mechanism in place to verify the installed software.

The audit team would like to acknowledge and thank management for its support throughout the conduct of this audit.

Appendix A: Audit Criteria

Line of Enquiry 1. **CNSC has governance and oversight structures in place to ensure that IT assets, owned and/or consumed by the CNSC, are managed appropriately and comply with Government of Canada and CNSC policies.**

1.1. A management structure is in place which defines accountability for IT assets both owned and consumed by the CNSC.

1.2. Roles and responsibilities are clearly defined and communicated.

1.3. Policies are developed for the management of IT assets both owned and consumed by the CNSC.

Line of Enquiry 2. **Processes and controls are in place for planning, acquiring, using (i.e., maintenance, replacement) and disposing of IT assets owned by the CNSC.**

2.1. The CNSC has a plan for acquisition, replacement, and disposal of IT assets.

2.2. Processes and procedures are in place for acquisition, replacement, and disposal of IT assets.

2.3. IMTD complies with CNSC and Treasury Board policies for acquisition and disposal of IT assets.

2.4. IMTD has developed and implemented hardware and software guidance for procurement.

2.5. The CNSC mitigates the risk of employees benefiting from the purchase and disposal of IT assets.

Line of Enquiry 3. **Processes and systems are in place to record, track, monitor and safeguard the IT assets owned by the CNSC.**

3.1. An asset tracking system is in place for IT assets and access is restricted to authorized staff.

3.2. IT assets records and information are accurate and complete, and periodically verified to ensure assets have not gone missing.

3.3. IT asset inventories are properly safeguarded when not in service, or scheduled for disposal.

3.4. IT assets identified for disposal follow the TB directive for disposal and are removed from the tracking system.

3.5. Sufficient software licences exist for the number of active users.

Appendix B: Audit Recommendations and Management Action Plan

The following table presents a summary of the recommendations and management action plans (MAPs) raised in section 2 (Audit observations and recommendations) of the report:

Action owner (office of primary interest)	**Management response and action plan**	**Timeline**
Recommendation 1. It is recommended that: a. a directive and written procedures be developed to describe practices that will be used in managing IT services b. roles and responsibilities be improved by i) defining, documenting and communicating the roles and responsibilities with respect to management of IT services. ii) segregating the Asset Management Group role into two separate functions: • asset recording • handling of inventory c. IMTD develop and implement practices to be used until an SLA is entered into with SSC		
	Recommendation 1 a. Management supports the recommendation. **Shared Services Canada – CNSC Interactions Standard for Telecommunications Services – e-Doc 4995600** – In order to address the recommendation, a new standard was created. Specifically, the new standard defines the demarcation of SSC and CNSC	Completed[1]

Action owner (office of primary interest)	Management response and action plan	Timeline
	responsibilities for services provided by SSC, along with service targets. This standard was written by the Information Management Division in consultation with the Telecommunications and Asset Management Officer. It was reviewed and approved by the SSC coordinator; the director, Information Technology Security and Services Division; and the director general, IMTD. This new standard document was sent by email to the parties involved on June 22, 2016. **Sep. 21, 2016 – Update** Document includes reference to satellite phones as a service. Referencing procurement of SSC services (e.g., networking, applications and email), SSC has not provided adequate visibility to departments / agencies to demonstrate the cost and/or value of the services. As a result, they have not been included at this time.	
	Recommendation 1 b. i) Management supports the recommendation. **Shared Services Canada – CNSC Interactions Standard for Telecommunications Services – e-Doc 4995600** – In order to address the recommendation, a new standard was created. Specifically, the new standard defines the roles and responsibilities of SSC and the CNSC. This new standard was written by the Information	Completed[1]

Action owner (office of primary interest)	Management response and action plan	Timeline
	Management Division in consultation with the telecommunications and asset management officer. It was reviewed and approved by the SSC coordinator; the director, Information Technology Security and Services Division; and the director general, IMTD. This new standard document was sent by email to the parties involved on June 22, 2016. **Sep. 21, 2016 – Update** Document includes reference to satellite phones as a service. Referencing procurement of SSC services (e.g., networking, applications and email), SSC has not provided adequate visibility to departments / agencies to demonstrate the cost and/or value of the services. As a result, they have not been included at this time.	
	Recommendation 1 b. ii) Management supports the recommendation. **IT Asset Assignment & Tracking Procedures – e-Doc 3875336**. In order to address the recommendation, the procedure was amended. Specifically, the revised document now segregates duties between the asset management officer and the IT asset TSC technician in relation to asset recording and inventory handling. This revised procedure was reviewed and updated by the telecommunications and asset management officer and approved by the director, ITSSD. This revised	Completed[1]

Action owner (office of primary interest)	Management response and action plan	Timeline
	procedures document was sent to TSC on June 22, 2016 **Recommendation 1 c.** Management agrees with the recommendation. **Shared Services Canada – CNSC Interactions Standard for Telecommunications Services – e-Doc 4995600** – In order to address the recommendation, a new standard was created. Specifically, the new standard defines the demarcation of SSC and CNSC responsibilities for services provided by SSC, along with service targets. This standard was written by the Information Management Division in consultation with the telecommunications and asset management officer. It was reviewed and approved by the SSC coordinator; the director, Information Technology Security and Services Division; and the director general, IMTD. This new standard document was sent by email to the parties involved on June 22, 2016. **Sep. 21, 2016 – Update** Document includes reference to satellite phones as a service. Referencing procurement of SSC services (e.g., networking, applications and email), SSC has not provided adequate visibility to departments / agencies to demonstrate the cost and/or value of the services. As a result, they have not been included at this	Completed[1]

Action owner (office of primary interest)	Management response and action plan	Timeline
	time.	
Recommendation 2. It is recommended that: a. the draft policy suite-related documents, including procedures related to the Information Technology Asset Management Directive be updated, approved and communicated to all stakeholders b. procedures relating to service procurement be developed, approved, and communicated		
	Recommendation 2 a. Management agrees with the recommendation. **Asset Management Directive: e-Doc 3840611;** **IMTD Process – IT Asset Procurement: e-Doc 4999678; and** **IMTD Process – Wireless Device Requests: e-Doc 4984301** In order to address the recommendation, the Asset Management Directive was amended and asset procurement and management processes were created. Specifically, the revised directive's footer was properly updated to include accurate directive update and revision dates. The asset procurement and wireless devices processes were created to clarify roles and responsibilities. The updated directive was reviewed and approved by the CIO, and the processes were reviewed and approved by the director, ITSSD. The contents of these documents have been communicated to TSC staff as appropriate.	Completed[1] Completed[1]

Action owner (office of primary interest)	Management response and action plan	Timeline
	Recommendation 2 b. Management supports the recommendation. **IMTD Process – Wireless Device Requests – e-Doc 4984301** – In order to address the recommendation, a new process was created. Specifically, it describes the process to follow to obtain telecommunications services from SSC. The process was created by the Information Management Division in consultation with the telecommunications and asset management officer. It was reviewed and approved by the SSC coordinator and director, Information Technology Security and Services Division. This new process document was sent by email to the parties involved on June 22, 2016. **July 13, 2016 Update –** Document has been updated and renamed to Shared Services Canada (SSC) Service Procurement Procedures and includes documented procedures for videoconference and landline services. **Sep 21, 2016 – Update – CNSC Interactions Standard for Telecommunications Services – e-Doc 4995600** Document includes reference to satellite phones as a service. Referencing procurement of SSC services e.g. networking, applications and email),	

Action owner (office of primary interest)	Management response and action plan	Timeline
	SSC has not provided adequate visibility to departments / agencies to demonstrate the cost and/or value of the services. As a result, they have not been included at this time.	
Recommendation 3. It is recommended that lifecycle procedures and controls be improved by: a. developing, approving, and communicating the procedure for the acquisition of hardware and software b. revising current procedures to describe: i) items for disposal and their method of disposal ii) items for the Computers for School program and procedures for removing sensitive information from media c. documenting the process for IT disposition including the controls over tracking and safeguarding of surplus assets		
	Recommendation 3 a. Management agrees with the recommendation. **IMTD Process – IT Asset Procurement – e-Doc 4999678** – In order to address the recommendation, a new process document was created. Specifically, it outlines the procedures to be followed for the procurement of hardware and software. This process was written by the Information Management Division in consultation with the various groups involved in the procurement process. It was approved by the director, Information Technology Security and Services Division.	Completed[1]

Action owner (office of primary interest)	Management response and action plan	Timeline
	Recommendations 3 b. i) ii) Management agrees with the recommendation. **IT Asset Assignment & Tracking Procedures – e-Doc 3875336**. Item 4.5, Step 3. In order to address the recommendation, the procedures document was reviewed and amended. Specifically, it describes the method of disposal of equipment for the Computers for School program and the procedures for removing sensitive data before disposal. This revised procedure document was reviewed by the telecommunications and asset management officer and approved by the director, Information Technology Security and Services Division. This revised procedures document was sent to TSC staff on June 22, 2016. **Recommendation 3 c.** Management agrees with this recommendation **IT Asset Assignment & Tracking Procedures – e-Doc 3875336**. Item 4.17 – Asset Disposal. In order to address the recommendation, the procedures document was reviewed and amended. Specifically, it demonstrates the segregation of duties of all parties involved in the disposition of equipment including the controls over tracking and safeguarding of surplus assets.	Completed[1]

Action owner (office of primary interest)	Management response and action plan	Timeline
	This revised procedures document was reviewed and amended by the telecommunications and asset management officer and approved by the director, Information Technology Security and Services Division. This revised procedures document was sent to the TSC on June 22, 2016.	Completed[1]
Recommendation 4. It is recommended that the asset tagging procedures and controls be improved by: a. placing an asset tag on all CNSC assets b. having the TSC technician tag all newly acquired assets before they are placed in the inventory c. removing or obliterating asset tags on assets transferred to SSC d. procuring asset tags that can withstand wear e. collecting assets considered obsolete and ensuring disposition takes place		
	Recommendation 4 a. Management agrees with the recommendation. All CNSC assets must have an asset tag, space permitting. Certain assets such as e-tokens do not permit an asset tag to be tagged given the lack of physical space. In these circumstances, the serial numbers are used to track the devices. **Recommendation 4 b.** Management agrees with the recommendation. **IT Asset Assignment & Tracking Procedures – e-Doc 3875336.** Item 4.10 – Receiving and Tagging Assets. In order to	Completed[1] Completed[1]

Action owner (office of primary interest)	Management response and action plan	Timeline
	address the recommendation, the procedures document was reviewed and amended. Specifically, it demonstrates the segregation of duties between the IT asset management officer and the IT asset TSC technician for the receiving and tagging of new equipment. This revised procedures document was reviewed and amended by the telecommunications and asset management officer and approved by the director, Information Technology Security and Services Division. Additionally, this revised procedures document was communicated to implicated parties. This revised procedures document was sent to ITSSD parties on June 22, 2016. **Recommendation 4 c.** Management agrees with this recommendation. CNSC tags will be removed from SSC IT assets by June 2016. **Recommendation 4 d.** Management agrees with this recommendation. In 2012, inferior quality tags were purchased, which resulted in premature wear of the tags. IMTD now uses more robust asset tags that can withstand wear. **Recommendation 4 e.** Management agrees with this recommendation.	Completed[1]

Action owner (office of primary interest)	Management response and action plan	Timeline
	In order to address the recommendation, an email was sent to users for the recall of the old USB keys. All but two USB keys have been returned. Follow-up emails were sent with cc to Management. Disposal for destruction is done on a yearly basis. USB keys will be sent on next destruction shipment at the end of the fiscal year. **October 4, 2016 – Update** IMTD has confirmed with the employee that no personal or sensitive information was saved on the USB keys. The 2 outstanding USB keys have been returned, as a result, no further action is required.	Completed[1]
Recommendation 5. It is recommended that: a. a study should be conducted of the COTS system to determine which functionality is missing or not functioning, as required, and corrective action should be taken b. the process and associated procedures be improved to accurately reflect which assets are under CNSC management by clearly marking items with asset tags and accurately reflecting the asset in the asset management system		
	Recommendation 5 a. Management agrees with the recommendation. Shared Services has recently released a Request for Information (RFI) in order to obtain a government-wide solution for IT asset management. IMTD will conduct an analysis of the existing COTS system to identify missing	Completed[1]

Action owner (office of primary interest)	Management response and action plan	Timeline
	functionality. The outcomes of the study will be used to determine whether SSC IT asset management fully meets our requirements. If not, we will acquire a suitable replacement. **Oct. 4 – Update** IMTD has completed the analysis of the COTS system and the requirements have been incorporated into the IMTD service management tool assessment. Procurement is expected to occur in fiscal year 2017–18. **Recommendation 5 b.** Management agrees with the recommendation. **IT Asset Assignment & Tracking Procedures – e-Doc 3875336.** Appendix A – Tagged and Excluded Items List. In order to address the recommendation, the procedures document was amended. Specifically, appendix A shows the CNSC items that are to be tagged and items that are tracked by serial numbers. This revised procedures document was reviewed and amended by the telecommunications and asset management officer and approved by the director, Information Technology Security and Services Division. This revised procedures document was sent to TSC on June 22, 2016.	Completed[1]
Recommendation 6. It is recommended that:		

Action owner (office of primary interest)	Management response and action plan	Timeline
a. the accuracy of assets be improved by: i) having all assets verified during the annual verification and the loaner pool inventories verified on a more frequent basis ii) implementing software licensing verification tool iii) periodically obtaining telecommunications asset information from SSC and verifying it against CNSC-collected information. b. steps be taken to locate assets missing during the inventory count that could contain sensitive business information		
	Recommendation 6 a. i) Management agrees with the recommendation. IMTD has implemented a mandatory monthly verification of the loaner pool for all devices. **July 13, 2016 Update –** IMTD conducts an annual verification of all CNSC IT assets. **Recommendation 6 a. ii)** Management agrees with the recommendation. Shared Services has recently released a Request for Information (RFI) in order to obtain a government-wide solution for IT asset management including a licencing software verification tool. Once procured by SSC, the CNSC will implement the tool. **Oct. 13, 2016 – Update** As an interim solution to SSC's enterprise	Completed[1] Q4 2016/17

Action owner (office of primary interest)	Management response and action plan	Timeline
	tool, IMTD will implement the licence compliance feature on the SCCM tool, which will track the number of software licences on the Production and Lab environment. **Recommendation 6 a. iii)** Management supports the recommendation. **IMTD Process – Wireless Device Requests – e-Doc 4984301** – In order to address the recommendation, a new process document was created. Specifically, the new standard includes the process to follow when ordering wireless services from SSC. Effective April 1 2016, IMTD receives and validates usage reports from SSC and verifies it against CNSC-collected information. This process was written by the Information Management Division in consultation with the telecommunications and asset management officer. It was reviewed and approved by the SSC coordinator and approved by the director, Information Technology Security and Services Division. This new process document was sent by email to the parties involved on June 22, 2016. **July 13, 2016 – Update –** Document has been updated and renamed to Shared Services Canada (SSC) Service Procurement Procedures and includes documented procedures for videoconference and landline services.	Completed[1]

Action owner (office of primary interest)	Management response and action plan	Timeline
	Recommendation 6 b. Management agrees with the recommendation. All assets identified in the audit were located and have been added to the inventory.	Completed[1]

Appendix C: Acronyms

CCTV	Closed circuit television
CFS	Computers for Schools program
CNSC	Canadian Nuclear Safety Commission
FAA	Financial Administration Act
IMTD	Information Management and Technology Directorate
IT	Information Technology
MAP	Management Action Plan
OAE	Office of Audit and Ethics
RBAP	Risk Based Audit Plan
SLA	Service Level Agreement
SSC	Shared Services Canada
TB	Treasury Board
TBS	Treasury Board Secretariat
TSC	Technical Service Centre
USB	Universal Serial Bus

Appendix D: Information Technology Assets Owned by or Entrusted to the CNSC

The following is a list of IT assets which IMTD uses to deliver IT services which were included in the audit.

Information technology assets included:

1. Hardware
   - Desktop workstations
   - Laptops
   - Tablets
   - Peripheral devices connected to the computers that include: printers, scanners, wireless broadband modems, removable media such as USB keys, portable hard drives, CDs, DVDs, etc.

2. Software
   - Standard operating system[2]
   - Standard workstations applications
   - Non-standard software desktop applications
   - Specialized scientific applications

3. Audio visual equipment
   - Videoconferencing/telepresence equipment[1]
   - TVs
   - Digital projectors
   - DVRs
   - Conference room phones

4. Network Infrastructure
   - Servers[2]
   - Routers[2]
   - Access points[2]
   - Modems[2]
   - Switches[2]
   - Hubs and bridges[2]
   - Cabling[2]

[2] Denotes IT assets owned by SSC and entrusted to CNSC.

5. Network software
   - Standard server operating system[2]

Technology assets included:

1. Landline and mobile telecommunications devices
   - Centrex landlines[2]
   - Cell phones[2]
   - Smart phones such as BlackBerry devices[2]
   - Satellite phones[2]

[2] Denotes IT assets owned by SSC and entrusted to CNSC.