Industry Canada Industrie Canada

Audit Report

Audit of Information Technology Asset Management

Audit and Evaluation Branch

April 2015

Recommended for Approval to the Deputy Minister by the Departmental Audit Committee on May 5, 2015

Approved by the Deputy Minister on May 13, 2015

Canada

This publication is also available online at: http://www.ic.gc.ca/eic/site/ae-ve.nsf/eng/h_03776.html

To obtain a copy of this publication or an alternate format (Braille, large print, etc.), please fill out the Publication Request Form at www.ic.gc.ca/Publication-Request or contact the:

Web Services Centre
Industry Canada
C.D. Howe Building
235 Queen Street
Ottawa, ON K1A 0H5
Canada

Telephone (toll-free in Canada): 1-800-328-6189
Telephone (Ottawa): 613-954-5031
TTY (for hearing-impaired): 1-866-694-8389
Business hours: 8:30 a.m. to 5:00 p.m. (Eastern Time)
Email: info@ic.gc.ca

Permission to Reproduce

Cat. No. Iu4-166/2015E-PDF
ISBN 978-0-660-02766-1

Aussi offert en français sous le titre *Audit de la gestion des biens de technologie de l'information.*

Table of Contents

List of Initialisms and Acronyms Used in Report

ADM	Assistant Deputy Minister
AEB	Audit and Evaluation Branch
CIO	Chief Information Office
CIPO	Canadian Intellectual Property Office
CMS	Corporate Management Sector
CSD	Corporate Services Directorate
DG	Director General
DSO	Departmental Security Officer
DSR	Desktop Software Renewal
GC	Government of Canada
HEAT	Helpdesk Expert Automation Tool
IC	Industry Canada
IFMS	Integrated Financial and Material System
IT	Information Technology
MS	Microsoft
OIC	Order In Council
ORBITT	Organizational Renewal and Business IT Transformation
PMM	Plant Maintenance Module
RCM	Responsibility Centre Manager
RVD	Request for Volume Discount
SITT	Spectrum, Information Technologies and Telecommunications Sector
SSC	Shared Services Canada
SSD	Security Services Directorate
TB	Treasury Board of Canada

1.0 Executive Summary

1.1 Background

In accordance with the approved Industry Canada (IC) 2014-15 to 2016-17 Multi-Year Risk-Based Internal Audit Plan, the Audit and Evaluation Branch (AEB) undertook an audit of Information Technology (IT) Asset Management.

The management of assets is directed by Treasury Board (TB) *Policy Framework for the Management of Assets and Acquired Services* and is complemented by additional TB direction addressing IT asset management. This includes the TB *Policy Framework for Information and Technology; Policy on the Management of Materiel*; Guide to Management of Materiel; Operational Security Standard on Physical Security; *Policy on Accounting for Inventories*; and the Directive on the Disposal of Surplus Materiel.

Accordingly, the Deputy Head of Industry Canada (IC) is accountable and responsible for implementing an effective management framework, including departmental procedures, processes, and systems that demonstrate how IC is managing its assets and for the effective management of information and technology throughout the Department. The Chief Financial Officer is accountable for ensuring an effective asset management framework is in place.

In support of meeting TB requirements, IC has implemented a framework for managing its assets (including IT assets) comprised of key departmental policies, procedures, processes such as the Asset Management Governance Structure; *Asset Management Policy*; *Software Asset Management Policy*; and the *Departmental Security Policy*.

In addition, IC uses the Plant Maintenance Module (PMM) within the Integrated Financial and Materiel System (IFMS) to record and track all barcoded assets within the Department including IT hardware assets. The total value of barcoded departmental IT hardware assets is not readily available from PMM as there is a lack of clear definition of what constitutes an IT hardware asset as further explained in section 3.2 of the report.

At IC, key roles and responsibilities in regard to IT asset management are as follows:

- Within the Corporate Management Sector (CMS):
  - ✓ The Corporate Finance, Systems, and Procurement Branch is the functional authority for the management of departmental assets.
  - ✓ The Contracts and Materiel Management (CMM) and Corporate Finance groups within this branch are responsible for providing functional direction, advice and guidance in all areas of the materiel management life cycle and lead the annual asset verification exercise.
  - ✓ The Security Services Directorate (SSD) is responsible for providing direction on the safeguarding of IC information and assets from compromise, and for investigating lost or stolen assets with collaboration from Chief Information Office (CIO), IT Security.

- The CIO Sector is responsible for providing direction and approval for the procurement of IT Products (hardware and software) and Services; coordinating the departmental Request for Volume Discount (RVD) procurement process for desktop computers and monitors; and, carrying out activities related to disposals, particularly data wiping and secure destruction.
- For each sector and branch:
    - ✓ Assistant Deputy Ministers and equivalents promote and support departmental initiatives related to asset management to ensure effective integration of roles and responsibilities for those involved in asset management activities within their respective organizations.
    - ✓ Responsibility Centre Managers, Asset Managers and Custodians are responsible for the day-to-day application of policies and procedures related to asset management (e.g. procurement, tracking of IT assets, annual asset verification, and disposals).

IT assets represent an essential component of the Government of Canada's (GC) strategy to address challenges related to increasing productivity and enhancing services to the public for the benefit of citizens, businesses, and employees. As such, IT is changing significantly across the GC. Major initiatives, such as the creation of Shared Services Canada (SSC), is a move towards the GC's objective of having a government-wide, standardized, centralized approach to managing its IT infrastructure, including supplying and supporting software and IT hardware assets. Two Orders in Council (OIC) were released in 2013 to authorize the transfer of duties from departments to SSC related to the acquisition and provision of hardware and software for end user devices. While the first OIC has been carried out, the second OIC which requires SSC to provide services for IT hardware and software assets is not yet implemented and IC is still managing its IT assets.

To incorporate these significant changes within its operational business environment, CIO senior management acknowledges the need of having a greater partnership between business units, the CIO and SSC. A longer-term priority of centralizing the management of IT hardware and software assets was also adopted by IC as a pre-cursor to the government-wide centralization approach.

The Department launched the Organizational Renewal and Business IT Transformation (ORBITT) initiative, which consolidated some IT resources from the Spectrum, Information Technologies and Telecommunications Sector (SITT) and the Canadian Intellectual Property Office (CIPO) within the CIO Sector. As part of this consolidation effective April 1st, 2014, the CIO became responsible for carrying out custodian services of some IT assets on behalf of CIPO and SITT.

Furthermore, the CIO has undertaken the Desktop Software Renewal (DSR) project to renew IC's aging desktop computer operating system and related software by April 2014. In parallel with the DSR project, in October 2013, the CIO took on the responsibility for procuring desktop software within the Department.

1.2 Audit Objective and Conclusion

The objective of the audit was to provide reasonable assurance that the IT asset management control framework is adequate. The key components examined during this audit included: processes in place to ensure compliance with key requirements outlined in IC and Government of Canada policies, directives and guidelines; understanding of roles, responsibilities and authorities; acquisition and tracking of IT assets; and disposal activities.

The scope of the audit included IT hardware and software assets and covered activities during the period of April 2013 to February 2015.

The results of the audit revealed that while the Department manages its IT assets through an IT asset management control framework, weaknesses have been identified, with low to moderate risk exposures that require management attention. Improvements are required to address these risk exposures specifically in the areas of: governance; policies, directives, and guidance; activities and processes (e.g. CIO approval, software asset management, disposals); and consideration of the sensitivity of information on missing assets. In each of these areas, clarity of roles and responsibilities and better documented processes warrant timely consideration.

1.3 Main Findings and Recommendations

Governance

Roles, responsibilities, and accountabilities have changed on some aspects of IT asset management and are not reflected in the *Industry Canada Asset Management Governance Structure*. In addition, the assignment of these roles and responsibilities do not always take into consideration adequate segregation of duties.

Various IC initiatives, in support of the government-wide objective mentioned above in section 1.1, resulted in changes to the CIO's roles, responsibilities, processes, and activities it carries out.

- The DSR project provided the CIO with an opportunity to develop new processes, activities, and supporting tools regarding software procurement and management.
- In October 2013, the CIO took on the responsibility for procuring desktop software within the Department.
- In addition, the CIO created a baseline inventory listing of software on IC staff computers.

The audit found that while some business units continue to collect and record information of software purchases (including licenses); others believe that this responsibility was transferred to the CIO when they created the baseline inventory listing of software. There is confusion among some IC staff in relation to their roles and responsibilities as they pertain to software tracking.

Information on roles, responsibilities and accountabilities regarding disposal activities for IT hardware assets, including secure destruction, is not reflected in the *Asset Management Governance Structure* document. In addition, the audit found that some roles, responsibilities

and accountabilities associated with secure destruction do not take into consideration adequate segregation of duties.

Recommendation 1:

a) CMS should ensure that during their three-year review cycle this fiscal year, the *Asset Management Governance Structure* document is updated to to reflect the current roles and responsibilities of all internal stakeholders and re-align, where needed, some roles and responsibilities, acknowledging adequate segregation of duties.
b) CMS, in collaboration with the CIO, should communicate these updates to IC staff.

There are review processes in place to update IC policies, directives, procedures and guidelines. The documents, however, do not reflect current practices. As a result, some of them are outdated and gaps exist.

The audit found that changes related to IT asset management and procurement were not reflected in neither CMS nor CIO policies, directives, procedures and guidelines. Current governing documents are outdated and some gaps exist. As well, it was unclear how CMS and CIO collaborate for the purpose of meeting client needs in the field of IT asset management.

CMS confirmed that they will review and update their policies and directives during 2015-16, as part of their established three year review cycle. Within the CIO, the review and update process of their specific governing documents occurs on an as needed basis. CIO's intention is to update them as soon as it is feasible.

Recommendation 2:

a) CMS should ensure that during their three-year review cycle this fiscal year, departmental policies, directives and guidelines related to IT asset management are updated, in collaboration with CIO, to better support IC staff in fulfilling their roles and responsibilities.
b) CIO should ensure that its specific governing documents related to IT asset management and procurement are updated in 2015-16, in collaboration with CMS, to better support IC staff in fulfilling their roles and responsibilities.
c) CMS and CIO should consider synchronizing their review processes so that information related to IT asset management is being updated on a regular basis and at the same time.

Procurement

Computers and monitors are purchased through the mandatory Request for Volume Discount (RVD). Justifications are provided when these purchases do not go through this process.

The audit found that these purchases were in accordance with the CIO *Directive on the IT Products and Services Procurement Process,* which states that IC staff must use the mandatory

RVD process to purchase planned and regular desktop computers and monitors or provide a rationale as to why the purchase could not go through the RVD process.

The CIO approval process is still being defined, documented, and communicated.

The CIO *Directive on the IT Products and Services Procurement Process* describes the Department's process for the approval of procurement of IT products. According to this directive, IC staff needs to seek CIO approval prior to the procurement of non-RVD desktop computers and monitors, other IT hardware assets, as well as the procurement of software.

The audit found instances where no CIO approval was sought prior to the procurement of the IT asset. As well, IC staff was not always aware of the CIO approval requirement and was unclear as to what types of IT assets require CIO approval. The audit found that there is no clear departmental definition of what constitutes an IT hardware asset and would require a CIO approval. In addition, for software assets, there was insufficient guidance that explains what types of software are subject to the CIO approval.

Also, the audit found that, although in some instances where CIO approval was obtained prior to the purchase of the IT hardware or software, the process was not consistently followed as the request for CIO approval was made through e-mail or verbally, instead of using the E-Request form which was in effect during the period of the audit.

The CIO approval process has evolved over time with the implementation of E-Request forms to seek approval, the Helpdesk Expert Automation Tool (HEAT) Ticket System to track and manage CIO approval requests and status, and the creation of various IT analysis groups. To reflect these changes, the CIO is currently drafting an internal document titled IT Approval Process.

Recommendation 3: The CIO should:

a) Complete drafting their internal procedures and reflect them in the IT Approval Process document and communicate it to CIO staff; and
b) Improve its governing documents related to the CIO approval process for the procurement of the IT hardware and software and communicate the changes to IC staff.

Tracking and Updating IT Asset in Management Systems

IT hardware assets are barcoded, tracked within the asset management system, and kept up-to-date through a combination of formal and ad-hoc activities.

The audit found that all IT hardware assets were barcoded and tracked in the PMM. In addition, updates of key information (e.g. changes of location and personnel) had occurred in the PMM for most of the IT hardware assets prior to the commencement of the annual asset verification exercise.

The annual asset verification exercise is conducted in accordance with departmental and Government of Canada requirements. As part of this exercise, the Department has implemented controls to mitigate the risks associated with some activities assigned to custodians. In addition, some good practices were adopted such as the use of a designated person to coordinate the exercise on behalf of all custodians within a business unit and then to liaise with CMS and the involvement of other IC staff to help provide independence from the custodian of the account.

The audit found that custodians are the ones carrying out the annual asset verification exercise and that most of the custodians performed both the inventory taking and record keeping functions. To compensate for this lack of segregation of duties, the Department has implemented controls within this exercise.

Not enough attention is given to the sensitivity of information on hardware assets with data storage capability declared as missing during the annual asset verification exercise.

The audit found that follow-up activities on IT hardware assets declared as missing do not include an assessment on the sensitivity of information stored on those with data storage capability. As well, no guidance exists as part of the annual asset verification exercise to assist IC staff on the need for such an assessment.

As a result, sensitive information that may exist on missing IT hardware assets with data storage capability would not be identified and appropriate follow-up steps would not be taken which is contrary to IC and GC requirements concerning the protection of information throughout its lifecycle.

Recommendation 4: CMS should update its documentation related to the annual asset verification exercise (including training material and procedures) to ensure attention is given by appropriate personnel to the sensitivity of information on missing IT assets with data storage capability.

The tracking of software is not performed consistently across the Department. Some initiatives have been undertaken to improve the monitoring of software installation.

The audit found that there is no common departmental IT asset management system to track software. As well, tracking of software, including licenses and renewals, by IC staff within the Department is not performed consistently.

In addition, the audit found that the CIO is tracking software for its own sector, SITT and CIPO, as well as for some departmental corporate software. CIO staff also stated that they are not responsible for tracking all software on behalf of the Department. CIO also acknowledged that the activities arising from the DSR project and the centralization of desktop software procurement within CIO have contributed to the confusion around software tracking responsibilities across the Department.

The CIO is creating a MS Access database to track and manage the CIO, SITT and CIPO's software in order to support activities related to procurement, license renewal, upgrades and

maintenance. In addition, activities are being undertaken to help mitigate the risk of exposure to potential liability by ensuring that legal ownership of software can be demonstrated.

Recommendation 5: CIO, in collaboration with CMS, should require that departmental software (including licenses and renewals) be tracked in a centralized database to ensure software tracking activities meet the operational needs.

Disposal Activities

Some aspects of the disposal process are still to be defined, including those activities related to the sensitivity of information and secure destruction.

A variety of disposal mechanisms are available to IC staff. The audit found that the Computer and Internet Access program was used by IC staff as the first option for disposal, which is consistent with both IC and TB requirements.

The IC Standards and Guidelines for Disposal of Surplus Electronic and Electrical Equipment identified the procedures to follow when disposing surplus IT assets. However, it does not always clearly explain how to document these activities. As such, evidence was not always available to demonstrate that the Responsibility Centre Managers (RCM) authorized the disposals. In addition, the assessment of sensitivity of information on IT assets with data storage capability, which would determine whether the IT asset needs to be wiped or destroyed, was not always documented by the RCM.

The audit also found that documented IC guidance regarding secure destruction was insufficient and unclear. There was variation in the manner in which requests were made for proceeding with secure destruction and IC staff was unclear on the process they were expected to follow, including whom to contact.

Recommendation 6: The CIO, in collaboration with CMS, should better define, document, and communicate the disposal process including those activities related to secure destruction and consideration of sensitivity of information.

Lost and Stolen IT Hardware Assets

Lost and stolen hardware assets are reported in a timely manner and the Department is working on refining its approach for assessing if sensitive information exists on these IT assets.

The audit found that identification and timely reporting of lost or stolen IT assets is promoted within IC as there are various channels through which the reporting of a lost or stolen IT asset can occur.

The audit also found that coordination occurs between CMS and the CIO regarding reported lost or stolen assets to ensure that appropriate SSD and CIO IT Security personnel are aware and

involved when needed. It was also noted that lost or stolen IT assets were reported and responded to by SSD within a week of the incident occurring.

1.4 Audit Opinion

In my opinion, while the Department manages its IT assets through an IT asset management control framework, there are weaknesses that have been identified. Improvements are required to address the low to moderate risk exposures specifically in the areas of governance; policies, directives, and guidance; activities and processes (e.g. CIO approval, software asset management, disposals); and consideration of the sensitivity of information. In each of these areas, clarity of roles and responsibilities and better documented processes warrant timely consideration.

1.5 Conformance with Professional Standards

This audit was conducted in accordance with the *Internal Auditing Standards* for the Government of Canada, as supported by the results of the Audit and Evaluation Branch's quality assurance and improvement program.

Brian Gear
Chief Audit Executive, Industry Canada

2.0 About the Audit

2.1 Background

In accordance with the approved Industry Canada (IC) 2014-15 to 2016-17 Multi-Year Risk-Based Internal Audit Plan, the Audit and Evaluation Branch (AEB) undertook an audit of Information Technology (IT) Asset Management.

The management of assets is directed by Treasury Board (TB) *Policy Framework for the Management of Assets and Acquired Services* and is complemented by additional TB direction addressing IT asset management. This includes the TB *Policy Framework for Information and Technology; Policy on the Management of Materiel*; Guide to Management of Materiel; Operational Security Standard on Physical Security; *Policy on Accounting for Inventories*; and the Directive on the Disposal of Surplus Materiel.

Accordingly, the Deputy Head of Industry Canada (IC) is accountable and responsible for implementing an effective management framework, including departmental procedures, processes, and systems that demonstrate how IC is managing its assets and for the effective management of information and technology throughout the Department. The Chief Financial Officer is accountable for ensuring an effective asset management framework is in place.

In support of meeting TB requirements, IC has implemented a framework for managing its assets (including IT assets) comprised of these key departmental policies, procedures, processes:

- Asset Management Governance Structure;
- *Asset Management Policy (POL 016);*
- *Software Asset Management Policy (POL 019);*
- *Departmental Security Policy;*
- Framework, Guidelines, and Procedures for the Annual Asset Verification Exercise;
- Directive on IT Products and Services Procurement Process;
- Draft IT Approval Process; and
- Guideline for the Disposal of Federal Surplus Electronic and Electrical Equipment.

In addition, IC uses the Plant Maintenance Module (PMM) within the Integrated Financial and Materiel System (IFMS) to record and track all barcoded assets within the Department including IT hardware assets. The total value of barcoded departmental IT hardware assets is not readily available from PMM as there is a lack of clear definition of what constitutes an IT hardware asset as further explained in section 3.2 of the report.

Key roles and responsibilities for IC staff involved in IT asset management and procurement activities are described below:

Corporate Management Sector (CMS):

- The Corporate Finance, Systems, and Procurement Branch is the functional authority for the management of departmental assets. This branch develops and communicates IC policies,

directives and procedures that comply with TB requirements, and maintains a central inventory database of departmental assets. The Contracts and Materiel Management (CMM) and Corporate Finance groups within this branch are responsible for providing functional direction, advice and guidance in all areas of the materiel management life cycle and lead the annual asset verification exercise.

- The Security Services Directorate (SSD) is responsible for providing direction on the safeguarding of IC information and assets from compromise, and for investigating lost or stolen assets with collaboration from Chief Information Office (CIO), IT Security.

The CIO Sector is responsible for: providing direction and approval for the procurement of IT Products (hardware and software) and Services; coordinating the departmental Request for Volume Discount (RVD) procurement process for desktop computers and monitors; and, carrying out activities related to disposals, particularly data wiping and secure destruction.

For each sector and branch:

- Assistant Deputy Ministers and equivalents promote and support departmental initiatives related to asset management (with support from DGs, Directors, Responsibility Centre Managers (RCMs), and Supervisors) to ensure effective integration of roles and responsibilities for those involved in asset management activities within their respective organizations.
- RCMs, Asset Managers and Custodians are responsible for the day-to-day application of policies and procedures related to asset management (e.g. procurement, tracking of IT assets, annual asset verification, and disposals).

IT assets represent an essential component of the Government of Canada's (GC) strategy to address challenges related to increasing productivity and enhancing services to the public for the benefit of citizens, businesses, and employees. As such, IT is changing significantly across the GC. Major initiatives, such as the creation of Shared Services Canada (SSC), is a move towards the GC's objective of having a government-wide, standardized, centralized approach to managing its IT infrastructure, including supplying and supporting software and IT hardware assets. Two Orders in Council (OIC) were released in 2013 to authorize the transfer of duties from departments to SSC related to the acquisition and provision of hardware and software for end user devices. While the first OIC has been carried out, the second OIC which requires SSC to provide services for IT hardware and software assets is not yet implemented and IC is still managing its IT assets.

To incorporate these significant changes within its operational business environment, CIO senior management acknowledges the need of having a greater partnership between business units, the CIO and SSC. A longer-term priority of centralizing the management of IT hardware and software assets was also adopted by IC as a pre-cursor to the government-wide centralization approach.

The Department launched the Organizational Renewal and Business IT Transformation (ORBITT) initiative, which consolidated some IT resources from the Spectrum, Information Technologies and Telecommunications Sector (SITT) and the Canadian Intellectual Property

Office (CIPO) within the CIO Sector. As part of this consolidation effective April 1st, 2014, the CIO became responsible for carrying out custodian services of some IT assets on behalf of CIPO and SITT.

Furthermore, the CIO has undertaken the Desktop Software Renewal (DSR) project to renew IC's aging desktop computer operating system and related software by April 2014. In parallel with the DSR project, in October 2013, the CIO took on the responsibility for procuring desktop software within the Department.

2.2 Objective and Scope

The objective of the audit was to provide reasonable assurance that the IT asset management control framework is adequate. The key components examined during the audit included:

- Processes in place to ensure compliance with key requirements outlined in IC and GC policies, directives and guidelines;
- Understanding of roles, responsibilities and authorities;
- Acquisition and tracking of IT assets; and
- Disposal activities.

The audit scope included IT hardware and software assets and covered processes and activities during the period of April 2013 to February 2015.

For the purpose of this audit, IT hardware assets were limited to the ones that were expected to be barcoded and tracked in the asset management system. According to IC's *Asset Management Policy*, these assets have a cost equal to or greater than $1,000 (excluding taxes), or are considered attractive in nature (even if less than $1,000). As well, the audit scope included IT assets expected to be approved by the CIO prior to purchase. The IT hardware assets include, for example, computers, monitors, laptops, printers, and tablets.

The audit scope also included IT software to be used on the departmental network, such as Microsoft Visio, Adobe Professional, and other software acquired to meet specialized or unique needs of a business unit within a sector or a branch.

The audit scope excluded IT professional services, hardware managed by SSC (e.g. Blackberries, telephones, and cell phones), and in-house developed software applications. As well, procurement activity addressed in the audit was limited to testing CIO's approval prior to the purchase of an IT asset and, therefore, excluded areas such as financial authorization, contracting, and payment activities. Furthermore, the scope related to the disposal activities was limited to administrative process requirements (e.g. the use of forms, approval of disposal), and excluded technical aspects of disposal (e.g. access control, facility design and capacity, physical storage, type of equipment).

2.3 Audit Approach

The audit was conducted in accordance with the *Internal Auditing Standards for the Government of Canada*. Sufficient and appropriate audit procedures have been conducted and evidence was gathered to support the accuracy of the conclusion and opinion provided and contained in this report. This opinion is based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed on with management. This opinion is applicable only to the areas examined and within the scope described herein.

The audit was performed in three phases: planning, conduct and reporting. A risk assessment was performed during the planning phase of this audit to confirm the audit objective and identify areas requiring more in-depth review during the conduct phase.

Based on the identified risks, AEB developed audit criteria that linked back to the overall audit objective. Appendix A lists these audit criteria with related audit results (e.g. met; not met; met with exceptions).

The approach adopted for gathering evidence on this audit included document review, interviews with IC staff having roles and responsibilities related to IT asset management, physical observations, and transaction testing. The sampling approach used to select transactions for control testing considered populations size, departmental coverage, and the level of evidence required to conclude on the overall audit criteria. As such, the type and size of samples selected within each process activity area (e.g. procurement; tracking; disposals) varied and the testing results are not representative of individual sectors, branches or business units. The samples selected covered the period of April 2013 to October 2014.

A debrief meeting was held with CMS and CIO management in March 2015 to validate the accuracy of the findings contained in this report and to discuss the recommendations.

3.0 Findings and Recommendations

3.1 Introduction

This section presents the audit findings that are based on evidence and analysis from the risk assessment and the execution of audit procedures.

In addition to the findings below, AEB has communicated to management, either verbally or in management letters, findings for consideration that were non-systemic, of low risk, or not directly related to the audit objective and criteria.

3.2 Governance

Roles, responsibilities, and accountabilities have changed on some aspects of IT asset management and are not reflected in the *Industry Canada Asset Management Governance Structure*. In addition, the assignment of these roles and responsibilities do not always take into consideration adequate segregation of duties.

The TB *Policy Framework for the Management of Assets and Acquired Services* defines roles, responsibilities and accountabilities of Deputy Heads related to asset management in departments. The policy states that Deputy Heads are responsible for implementing an effective management framework for asset management which includes IT asset management. As such, in July 2011, IC put into effect an *Asset Management Governance Structure* which defines roles, responsibilities, and accountabilities related to the management of assets.

During the course of the audit, we conducted document review and interviews to determine how the Department has defined asset management roles, responsibilities and accountabilities for its staff within the governance structure, as well as assess whether IC staff understands their roles and responsibilities.

Over the past two years, various IC initiatives, in support of the government-wide objective mentioned above, resulted in changes to the CIO's roles, responsibilities, processes, and activities it carries out. For example, the CIO has undertaken the Desktop Software Renewal (DSR) project to renew IC's aging desktop computer operating system and related software by April 2014. This provided the CIO with an opportunity to develop new processes, activities, and supporting tools regarding software procurement and management. For example, in October 2013, the CIO took on the responsibility for procuring desktop software within the Department. In addition, the CIO created a baseline inventory listing of software on IC staff computers. Furthermore, the Department launched the Organizational Renewal and Business IT Transformation (ORBITT) initiative, which consolidated some IT resources from the Spectrum, Information Technologies and Telecommunications Sector (SITT) and the Canadian Intellectual Property Office (CIPO) within the CIO Sector. As part of this consolidation effective April 1st,

2014, the CIO became responsible for carrying out custodian services of some IT assets on behalf of CIPO and SITT.

The audit found that even though the *Software Asset Management Policy* outlines responsibilities in relation to software tracking (i.e. resting with business units), and while some business units continue to collect and record information of software purchases (including licenses); there is a belief that this responsibility was transferred to the CIO when they created the baseline inventory listing of software. Consequently, there is still confusion among some IC staff in relation to their roles and responsibilities as they pertain to software tracking.

Furthermore, although information on roles, responsibilities and accountabilities regarding disposal activities, including secure destruction, of IT hardware assets is documented in various IC documents, these existing roles and responsibilities are not reflected in the *Asset Management Governance Structure* document. In addition, the audit found that some roles, responsibilities and accountabilities associated with secure destruction do not take into consideration adequate segregation of duties (e.g. record keeping and physical custody).

Currently, the *Asset Management Governance Structure* document does not reflect the new roles, responsibilities, and accountabilities that CIO took over within the Department such as the procurement of desktop software, and the custodial services on behalf of SITT and CIPO.

During the audit, CMS informed the audit team that a three-year review cycle is in place to review and update governing documents, such as the *Asset Management Governance Structure.* Therefore, this document will be updated during 2015-16 to reflect the current roles and responsibilities of all internal stakeholders and re-align, where needed, some roles and responsibilities.

Without clear, documented and communicated roles and responsibilities in relation to IT asset management activities (such as those that have changed within the CIO), there is a risk that these roles and responsibilities would not be clearly understood and performed.

Recommendation 1:

a) CMS should ensure that during their three-year review cycle this fiscal year, the *Asset Management Governance Structure* document is updated to reflect the current roles and responsibilities of all internal stakeholders and re-align, where needed, some roles and responsibilities, acknowledging adequate segregation of duties.
b) CMS, in collaboration with the CIO, should communicate these updates to IC staff.

There are review processes in place to update IC policies, directives, procedures and guidelines. The documents, however, do not reflect current practices. As a result, some are outdated and gaps exist.

To ensure compliance with TB *Policy Framework for the Management of Assets and Acquired Services*, which states that Deputy Heads are responsible for implementing procedures, processes and systems related to the management of assets, and for guiding IC staff in carrying out activities related to IT asset management and procurement, the Department has implemented policies, directives, procedures and guidelines. In addition to the *Asset Management Governance Structure* document, the main IC governing documents reviewed in the context of this audit include the following:

- *Asset Management Policy*, including Appendices A and B (POL 016) (July 2011);
- *Software Asset Management Policy* (POL 019) (July 2011);
- *Departmental Security Policy* (October 2006);
- Framework, Guidelines, and Procedures for the Annual Asset Verification Exercise (various dates - November 2010 through August 2014);
- *Directive on IT Products and Services Procurement Process* (July 2012);
- Draft IT Approval Process; and
- CMS *Materiel Management Policy* Framework - IC Standards and Guidelines for the Disposal of Surplus Electronic and Electrical Equipment (March 2012).

During the course of the audit, document review and interviews were conducted to assess whether IC policies, directives, procedures and guidelines are aligned with the GC requirements and that there is a process in place to review and update these documents.

In addition to the changes to roles and responsibilities previously mentioned, the audit found that more changes related to IT asset management and procurement have occurred, and are not reflected in neither CMS nor CIO policies, directives, procedures and guidelines. Through interviews, IC staff confirmed that these current governing documents are outdated and some gaps exist. The following are examples of outdated information and/or where gaps exist:

- The governing documents do not provide clear direction on what constitutes an IT asset or what is meant by IT asset management.
- IC's *Asset Management Policy* indicates that the Departmental Security Officer (DSO) is responsible for approving asset write-offs which is not the current practice. This activity is currently done by sector ADMs. In addition, this policy makes reference to the Authority for Removal of Materiel from Premises form; however, this form is no longer expected to be used.
- The *Directive – IT Products and Services Procurement Process* and Draft IT Approval Process document do not clearly describe which types of IT hardware and software assets need CIO approval, and which types of software are to be procured by the CIO rather than a business unit. These matters are addressed further in section 3.3 below.
- The IC's *Standards and Guidelines for the Disposal of Surplus Electronic and Electrical Equipment* refer to an electronic request form for secure destruction; however, this form does not exist.

IC staff stated that they rely on IC policies, directives, procedures and guidelines published on the intranet to obtain direction on asset management and procurement. In October 2014, CMS launched an Asset Management WIKI page to provide IC staff with the most current information on the asset management activities such as training material, presentations, practices and guidelines. This undertaking, however, did not provide IC staff with updated CMS and CIO governing documents. As well, the CIO is planning to update its intranet to provide better guidance on IT asset management and procurement. Through interviews, it was unclear how CMS and CIO collaborate for the purpose of meeting client needs in the field of IT asset management.

During interviews, IC staff described processes in place to review and update governing documents and assess the need for new ones. As previously mentioned within CMS, policies and directives are reviewed and updated on a three-year cycle basis. CMS confirmed that they will review and update their governing documents at the next scheduled review cycle planned to be conducted during 2015-16. Within CIO, the review and update process occurs on an as needed basis. CIO's intention is to update their documents as soon as it is feasible.

It is important to have consistent governing documents, with changes to roles, responsibilities and accountabilities reflected in the appropriate CMS and CIO policies, directives, procedures and guidelines. The combination of having outdated governing documents containing gaps increases the potential for non-compliance with IC and TB requirements, creates confusion and causes inefficiencies among IC staff.

Recommendation 2:

a) CMS should ensure that during their three-year review cycle this fiscal year, departmental policies, directives and guidelines related to IT asset management are updated, in collaboration with CIO, to better support IC staff in fulfilling their roles and responsibilities.
b) CIO should ensure that its specific governing documents related to IT asset management and procurement are updated in 2015-16, in collaboration with CMS, to better support IC staff in fulfilling their roles and responsibilities.
c) CMS and CIO should consider synchronizing their review processes so that information related to IT asset management is being updated on a regular basis and at the same time.

3.3 Procurement

Computers and monitors are purchased through the mandatory Request for Volume Discount (RVD). Justifications are provided when these purchases do not go through this process.

In 2001, IC adopted a mandatory Request for Volume Discount (RVD) process to collectively increase the value and power of the Department's IT spending dollar by obtaining better discounts for commodity IT purchases. This process is being led by the CIO for the regular planned purchase of desktop computers and monitors.

According to the CIO *Directive on the IT Products and Services Procurement Process*, IC staff must use the mandatory RVD process when purchasing planned and regular desktop computers and monitors. This process is initiated when the RVD Coordinator, within the CIO Corporate Services Directorate, conducts a mid-year and year-end call-out to business units who identify their needs, and coordinates the RVD procurement with the CIO's centralized asset management and purchasing groups. Then, the CIO procures desktop computers and monitors on behalf of IC sectors and branches. Once these IT assets are received, barcoded and recorded in the CIO custodial account within PMM, the CIO cost-recovers as the stock is transferred to the business units. As well, while it is currently not mandatory to purchase laptops through the RVD process, the CIO has taken steps to expand this RVD process to include laptops since 2013-14.

In situations where the RVD process could not be used, IC staff is allowed to purchase these desktop computers and monitors using the established procurement process in place. In these cases, a justification is required to provide rationale as to why the purchase could not go through the RVD process.

In the course of the audit, we performed transactions testing to assess whether the planned and regular desktop computers and monitors were purchased through the mandatory RVD process. We also examined whether a justification was documented when purchases of these types of IT assets occurred without using the RVD process.

The audit found that these computers and monitors were procured through the RVD process. Interviewees considered this process as a good practice and appreciated having someone within the sector or branch business unit coordinating the RVD and liaising with the CIO RVD Coordinator. In all circumstances when the purchases outside of the RVD process occurred, a justification for the procurement of these computers and monitors was documented. These purchases were mainly related to specific business operating needs that could not be postponed until the mid-year or year-end call-out events.

In addition, the audit results revealed that, in support of sound stewardship, most IC staff considered utilizing existing computers and monitors within their business unit prior to procuring these IT hardware assets.

The CIO approval process is still being defined, documented, and communicated.

In 2004, the CIO was designated as the principal IT advisor for the Department, including the responsibility for providing CIO approval before the procurement of IT products and services.

The objective for obtaining CIO approval prior to procurement of IT assets is to help determine whether the hardware will be compatible with IC's infrastructure, to understand whether there are any impacts for installation and servicing post-purchase, and whether the software will be acceptable on the IC network given security, licensing, and version considerations. This also provides the CIO with an opportunity to find out if the requested IT asset or software license is

currently available within other business units across the Department or if it needs to be procured.

The CIO *Directive on the IT Products and Services Procurement Process* describes the Department's process for the approval of procurement of IT products. According to this directive, IC staff need to seek CIO approval prior to the procurement of non-RVD desktop computers and monitors, IT hardware assets, as well as the procurement of software. This directive, in combination with the CIO's E-Request Instructional Guide, CIO approval E-Request forms, and other information available on the CIO's intranet provide guidance on the type of IT products that require CIO approval and the way to seek this approval.

The audit team performed document review, interviews and transaction testing to assess whether the CIO approval process was understood, followed and whether approval was obtained prior to the procurement of the IT hardware and software assets.

Based on the results of testing and interviews, there were instances where no CIO approval was sought prior to the procurement of the IT asset. In some of the instances, the audit found that IC staff were not always aware of the CIO approval requirement and were unclear as to what types of IT assets require CIO approval. For IT hardware assets, although the CIO Directive and related documents describe what requires CIO approval by listing examples, there is no clear departmental definition of what constitutes an IT hardware asset and would require a CIO approval. For example, guidance is needed to determine if assets such as projectors, televisions, USB keys, accessories, etc. are considered IT assets. In addition, for software assets, the audit found that there was insufficient guidance that explains what types of software are subject to the CIO approval (e.g. license renewals, on the network software, off the network software, specialized software, in-house developments).

During the audit, it was noted that the CIO was undertaking an initiative to update the CIO approval request forms for software to provide better guidance to IC staff on what types of software requires approval.

Also, the audit found that although in some instances where CIO approval was obtained prior to the purchase of the IT hardware or software, the process was not consistently followed as the request for CIO approval was made through e-mail or verbally, instead of using the E-Request form which was in effect during the period of the audit.

The CIO approval process has evolved over time with the implementation of E-Request forms to seek approval, the Helpdesk Expert Automation Tool (HEAT) Ticket System to track and manage CIO approval requests and status, and the creation of various IT analysis groups. To reflect these changes, the CIO is currently drafting an internal document titled IT Approval Process.

Given that the internal procedures on the IT Approval Process are still being drafted, CIO staff may not clearly understand and fulfill their roles and responsibilities associated with the CIO approval process which increases the risk of non-compliance with IC's directive.

In addition, without clear guidance on the CIO approval process, IC staff may not adequately understand and follow the process. As a result, they may procure IT hardware and software assets that would not be compatible with IC enterprise infrastructure and/or other products, negatively impact on the departmental network performance, IT support, and IT security risks may not be identified and mitigated.

Recommendation 3: The CIO should:

a) Complete drafting their internal procedures and reflect them in the IT Approval Process document and communicate it to CIO staff; and
b) Improve its governing documents related to the CIO approval process for the procurement of the IT hardware and software and communicate the changes to IC staff.

3.4 Tracking and Updating IT Asset in Management Systems

3.4.1 IT Hardware

IT hardware assets are barcoded, tracked within the asset management system, and kept up-to-date through a combination of formal and ad-hoc activities.

The TB *Policy on the Management of Materiel* states that Deputy Heads are responsible for ensuring that a materiel management information system is in place which enables the collection and generation of complete and accurate data on materiel asset holdings. Accordingly, IC has established the *Asset Management Policy* which requires that IT hardware assets with a cost equal to or greater than $1,000 (excluding taxes) or are considered attractive in nature (even if less than $1,000) must be recorded and tracked in the asset management system. IC uses the PMM within IFMS as its asset management system to record and track these assets throughout their lifecycle.

In the course of the audit, we performed document review, interviews, physical observations and transaction testing to determine whether IT hardware assets were barcoded, tracked and updated within the PMM.

The audit found that all IT hardware assets were barcoded and tracked in the PMM. In addition, updates of key information (e.g. changes of location and personnel) had occurred in the PMM for most of the IT hardware assets prior to the commencement of the annual asset verification exercise.

The annual asset verification exercise is conducted in accordance with departmental and Government of Canada requirements. As part of this exercise, the Department has implemented controls to mitigate the risks associated with some activities assigned to custodians. In addition, some good practices were adopted.

The TB *Policy on Accounting for Inventories* states that there is a need to conduct physical counts of inventory and that these counts should be performed, summarized, and verified with inventory records by persons who are independent from the inventory custodians.

IC's *Framework for the Annual Asset Verification Exercise* has been developed to establish roles and responsibilities, and to provide operational procedures on how IC staff are expected to conduct this exercise. This document requires that, once every fiscal year, a physical verification of its barcoded assets is conducted to ensure sound stewardship. The annual verification exercise is directed and coordinated by CMS. In addition, it defines an Inventory Taker as a person designated by the Sector or Regional Coordinator to complete the physical verification of assets. Normally, this activity falls to the custodian who carries out the physical count of IT hardware assets, updates key information in PMM (e.g. description of the asset, location), and when necessary, identifies and follows-up on missing assets and reports the results of the exercise to CMS.

During the audit, we performed document review and interviews to assess whether the annual asset verification exercise is conducted in accordance with departmental and GC requirements.

The audit found that custodians are the ones carrying out these activities as indicated in IC procedures and that most of the custodians performed both the inventory taking and recordkeeping functions. To compensate for this lack of segregation of duties, the Department has implemented controls within the annual asset verification exercise. These controls include: (1) limited custodian user access rights within the PMM preventing the creation and deletion of an IT asset's record; (2) requirement for custodian's signature on the reported results of the annual asset verification exercise submitted to CMS; and (3) requirement for ADM approval of writing-off IT assets declared missing.

Through interviews, the audit team identified some good practices that have been adopted by some sectors or business units with regards to this exercise. These include: (1) the use of a designated person to coordinate the exercise on behalf of all custodians within a business unit and then to liaise with CMS; (2) the use of hand-held scanners, tablets, and MS Excel tools (macros) to help improve the efficiency, accuracy and completeness of the inventory taking; and (3) the involvement of other IC staff to help provide independence from the custodian of the account. As well, the audit team noted that some custodians used a standardized naming convention as a good practice to record the physical location of an IT asset and to whom it is assigned.

Not enough attention is given to the sensitivity of information on hardware assets with data storage capability declared as missing during the annual asset verification exercise.

The TB *Directive on Departmental Security Management*, the TB *Operational Security Standard on Physical Security*, and IC's *Departmental Security Policy* require that information on IT assets be protected throughout its lifecycle which includes information that resides on IT assets with data storage capability.

During interviews, custodians confirmed that follow-up activities on IT hardware assets declared as missing do not include an assessment of the sensitivity of information stored on those assets with data storage capability. Through document review, the audit team found that no guidance exists within the *Framework for the Annual Asset Verification Exercise* to assist IC staff on the need for such an assessment. This exercise can be further strengthened to consider the sensitivity of information on missing IT assets with data storage capability. Custodians identified that this consideration would be a good practice.

As a result, sensitive information that may exist on missing IT hardware assets with data storage capability would not be identified and appropriate follow-up steps would not be taken which is contrary to IC and GC requirements concerning the protection of information throughout its lifecycle.

Recommendation 4: CMS should update the documentation related to the annual asset verification exercise (including training material and procedures) to ensure attention is given by appropriate personnel to the sensitivity of information on missing IT assets with data storage capability.

3.4.2 IT Software

The tracking of software is not performed consistently across the Department. Some initiatives have been undertaken to improve the monitoring of software installation.

The Department's *Software Asset Management Policy* outlines the expectations related to the management and use of software products and licenses. For example, custodians are responsible for keeping a central repository of software including licenses.

Within the Department, certain IC staff are granted enhanced user rights (e.g. software developers, engineers), which as part of their duties, allows them to download, install, and update software on their computer without CIO authorization.

In the course of the audit, we performed document review and interviews to determine whether software was tracked within the Department.

The audit found that there is no common departmental IT asset management system to track software. As well, tracking of software, including licenses and renewals, by IC staff within the Department is not performed consistently:

- Some do not track software and are not aware of this requirement.
- Some have stopped tracking software because they believe the CIO is tracking software and licenses for the entire Department since the DSR project took place.
- Some still track software and licenses for their own operational needs, within their business units, using various tools (e.g. MS Excel, Word, Access database).

Through interviews, CIO staff stated that their sector is responsible for tracking software for their own sector, SITT and CIPO, as well as for some departmental corporate software (e.g. Antidote). CIO staff also stated that they are not responsible for tracking all software on behalf of the Department. CIO also acknowledged that the activities arising from the DSR project and the centralization of desktop software procurement within CIO have contributed to the confusion around software tracking responsibility across the Department.

Currently, the CIO is creating a MS Access database to track and manage the CIO, SITT and CIPO's software in order to support activities related to procurement, license renewal, upgrades and maintenance. Interviewees mentioned that some activities are being undertaken to help mitigate the risk of exposure to potential liability by ensuring that legal ownership of software can be demonstrated:

- CIO is planning to update this database and some of its tools and processes (e.g. periodic comparisons between the MS Access database and what software is installed on IC staff workstations) to enhance the tracking of all departmental software products; and
- CIO also noted that there are tools in place to monitor the installation of unauthorized software by IC staff (including those with enhanced user access rights), detect malicious software, and identify unauthorized modifications to enhanced user groups.

The inconsistencies in current software tracking processes, along with limited communication on this subject, and the lack of centralized software tracking system might cause IC to not be able to support and account for the legal ownership of software used within the Department.

Recommendation 5:
CIO, in collaboration with CMS, should require that departmental software (including licenses and renewals) be tracked in a centralized database to ensure software tracking activities meet the operational needs.

3.5 Disposal Activities

Some aspects of the disposal process are still to be defined, including those activities related to the sensitivity of information and secure destruction.

In support of the TB *Directive on Disposal of Surplus Materiel* and the PWGSC Guideline for the Disposal of Surplus Federal Electronic, Electrical Equipment (EEE), the Department developed the following key documents to better guide IC staff on the disposal of IT assets:

- CMS *Materiel Management Policy* Framework - IC Standards and Guidelines for the Disposal of Surplus Electronic, Electrical Equipment (IC Standards and Guidelines for EEE); and
- Security Services Directorate's Guide to the Handling, Storage and Destruction of Protected and Classified Information.

Accordingly, a variety of disposal mechanisms are available to IC staff such as: (1) Computer and Internet Access program (formerly named the Computers for Schools program); (2) transfer to another federal department or agency; and (3) electronic waste. The IC Standards and Guidelines for EEE list the responsibilities of RCMs, examples of which include, identifying the level of sensitivity of data stored in the surplus equipment, and authorizing the custodian to process the disposal.

The audit team performed document review, interviews and transactions testing to assess whether the disposal is performed in accordance with IC and Government of Canada requirements.

The audit found that the Computer and Internet Access program was used by IC staff as the first option for disposal, which is consistent with both IC and TB requirements.

In addition, although IC Standards and Guidelines for EEE identified the procedures to follow when disposing surplus IT assets, it does not always clearly explain how to document these activities. For example, the procedures require RCMs to authorize disposals and to assess the sensitivity of information stored in surplus equipment. However, these procedures do not guide RCMs on how to document both of these requirements.

As such, evidence was not always available to demonstrate that RCMs authorized the disposals. In addition, the audit found that IC staff relies upon the CIO to wipe or sanitize the IT asset of data and identify when destruction is required if wiping is not possible. However, the assessment of sensitivity of information on IT assets with data storage capability, which would determine whether the IT asset needs to be wiped or destroyed, was not always documented by the RCM.

Transaction testing results demonstrated that various disposal forms were used and that they differed in their content in terms of certification statements and who was expected to sign-off. To address these inconsistencies, standardized forms were developed and communicated to IC staff during the course of the audit.

Audit test results showed that documented IC guidance regarding secure destruction was insufficient and unclear. There was variation in the manner in which requests were made for proceeding with secure destruction and IC staff was unclear on the process they were expected to follow, including whom to contact. Examples include: lack of clarity on which IT assets require secure destruction regardless of whether or not they can be sanitized; and insufficient guidance on what type of information to record, how, and to whom it should be provided, including packaging and shipping instructions.

Without sufficient and clear documented processes on disposal activities, including secure destruction, there is a risk that IT assets might not be properly disposed. In addition, sensitive information may not be identified and properly handled if the RCM assessment is not carried out.

Recommendation 6: The CIO, in collaboration with CMS, should better define, document, and communicate the disposal process including those activities related to secure destruction and consideration of sensitivity of information.

3.6 Lost and Stolen IT Hardware Assets

Lost and stolen hardware assets are reported in a timely manner and the Department is working on refining its approach for assessing if sensitive information exists on these IT assets.

As specified in the Department *Values and Ethics Code* and IC *Departmental Security Policy*, IC staff is responsible for the protection of IC information and assets. Within CMS, the SSD is responsible for providing direction on the safeguarding of information and assets from compromise, and for investigating lost or stolen assets with collaboration from the CIO, IT Security.

During the course of the audit, we performed document review, interviews, and transaction testing to assess whether IC staff understand to whom and when to report lost and stolen IT hardware assets, as well as to assess whether consideration is given to the potential sensitivity of information on such assets.

The audit found that identification and timely reporting of lost or stolen IT assets is promoted within IC as there are various channels through which the reporting of a lost or stolen IT asset can occur. The audit also found that coordination occurs between CMS and the CIO regarding reported lost or stolen assets to ensure that appropriate SSD and CIO IT Security personnel are aware and involved when needed. Based on the results of transaction testing, the audit found that lost or stolen IT assets were reported and responded to by SSD within a week of the incident occurring.

The audit found the enquiry regarding the sensitivity of information was not always documented by IC staff, including SSD. As such, we found that in some instances, no evidence was provided to demonstrate that the potential sensitivity of the information on a lost or stolen IT asset was considered.

During the audit, the SSD introduced, in August 2014, the use of a standardized questionnaire prior to carrying out an investigation on any lost or stolen asset. This document includes a question on the sensitivity of information by asking the existence and level of classified or protected information on lost or stolen assets. SSD is planning to improve its approach by asking IC staff to describe the type of information contained on the asset in order to help identify and document the consideration made regarding the sensitivity of information.

3.7 Management Response and Action Plan

The findings and recommendations of this audit were presented to the Corporate Management Sector (CMS) and the Chief Information Office (CIO) senior management. Management has agreed with the findings included in this report and will take actions to address most of the recommendations by March 2016, with the exception of one part of recommendation #5, by March 31, 2017 as it involves SSC.

The CMS and CIO, collaboratively, will review and update their governing documents (e.g. governance structure, policies, directives, procedures, guidelines) related to IT asset management to address some gaps and reflect the current practices. They will also communicate the updated documents through IC newsletters and intranet site to IC staff to better support them in fulfilling their roles and responsibilities.

In relation to the software tracking activities, they will collaboratively work on putting a centralized database in place and will require that departmental software be tracked in it.

4.0 Overall Conclusion

The results of this audit revealed that while the Department manages its IT assets through an IT asset management control framework, weaknesses have been identified, with low to moderate risk exposures that require management attention. Improvements are required to address these risk exposures specifically in the areas of governance; policies, directives, and guidance; activities and processes (e.g. CIO approval, software asset management, disposals); and consideration of the sensitivity of information. In each of these areas, clarity of roles and responsibilities and better documented processes warrant timely consideration.

Appendix A: Audit Criteria

Governance	Criteria Met/ Met with Exception(s)/ Not Met
1. IC policies, directives and guidelines exist, and are regularly reviewed and updated to ensure alignment with Departmental and Government of Canada requirements.	Met with exceptions
2. Roles, responsibilities and authorities are understood.	Met with exceptions
3. There is an appropriate segregation of duties in place.	Met with exceptions
Procurement	
4. IT asset procurement follows Departmental processes and requirements.	Met with exceptions
Management	
5. IT assets are tracked based on the established Industry Canada requirements and are properly updated within the asset management system.	Met with exceptions
6. IT asset disposals follow Industry Canada and Government of Canada requirements, with consideration given to useful life.	Met with exceptions
7. There is a process in place to identify missing, lost or stolen IT assets in a timely manner, and take appropriate corrective action to reduce associated risks.	Met with exceptions