Canada's Nuclear Regulator

Audit of IT Asset Management Report

Office of Audit and Ethics

July 10, 2012

Recommended by the Departmental Audit Committee for approval by the President on July 10, 2012

Approved by the President on September 4, 2012

e-Doc : 3854899

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Canada

Table of Contents

EXECUTIVE SUMMARY 3

1. INTRODUCTION 5

1.1. BACKGROUND 5
1.2. OBJECTIVE AND SCOPE 6
1.3. ANALYSIS OF RISKS AND AUDIT CRITERIA 7
1.4. APPROACH AND METHODOLOGY 7
1.5. STATEMENT OF ASSURANCE 8

2. OBSERVATIONS AND RECOMMENDATIONS 8

2.1. GOVERNANCE STRUCTURE 8
2.2. ACQUISITION, REPLACEMENT AND DISPOSAL OF ASSETS 9
2.3. MANAGEMENT OF IT ASSETS 12

3. INVENTORY TESTING 16

4. OVERALL RECOMMENDATION 18

5. OVERALL CONCLUSION 18

APPENDIX A – DETAILED AUDIT CRITERIA 19

APPENDIX B – OVERVIEW OF AUDIT RECOMMENDATIONS AND MANAGEMENT RESPONSE AND ACTION PLANS (MAP) 20

Executive Summary

Background

Information technology (IT) plays an important role in CNSC operations, and represents an essential component of the organization's strategy to address challenges of increasing productivity and enhancing mandated services for the benefit of citizens, businesses and employees.

Due to the growth in activities related to the nuclear sector, the CNSC has recruited a number of highly skilled professionals in the scientific, technical and administrative fields. Over the past four years, in order to meet this expansion in the number of full-time staff members, the CNSC has made several investments in IT hardware and software.

Since these represent attractive and important assets, an independent examination of the accuracy and completeness of the inventory and records was proposed to management. This audit was approved in the *CNSC Risk-Based Audit Plan* for 2011–14.

Objective and Scope

The objectives of the audit were the following:

- To determine whether adequate and effective IT asset management processes and controls are in place, in order to maintain the integrity of the IT assets while meeting the CNSC's and Government of Canada's requirements.
- To provide management with assurance that the IT asset inventory and records are complete and accurate.

The scope of the audit was limited to CNSC's information technology hardware and software inventories, including IT asset management practices in place as of July 2011. The audit's focus was on systems and practices used in the governance, management, control and oversight of IT hardware and software assets.

The audit testing excluded:

- Laptops: An inventory test count for laptops was included in the terms of reference (TOR) for this audit. However, at the time of the audit, the Information Management and Technology Division (IMTD) had not completed their inventory count of laptops, and could not provide a final list. The CNSC may decide to have the laptops subjected to a future audit.
- Telecommunication equipment (such as Blackberries and cellular telephones) was not included in the TOR for this audit. The CNSC President requested that an audit of this equipment be conducted. Therefore, the OAE plans to table an

audit of mobile telecommunication equipment at the July 2012 Audit Committee meeting.

- For logistical reasons, the inventory audited did not include the regional offices.

Approach and Methodology

The planned approach was to review documentation and interview key employees and managers, in order to identify the risks associated with IT asset management and to assess whether controls are in place to mitigate the risks.

The audit methodology included:

- Conducting interviews with managers and staff.
- Reviewing relevant CNSC and Government of Canada documents (including legislation, regulation, policies, directives, processes and procedures).
- Conducting tests on the accuracy of IMTD‘s inventory of IT assets.

The audit was conducted within the established parameters of the Treasury Board *Policy on Internal Audit,* as well as the *Auditing Standards* for the *Government of Canada*.

Audit Findings

The audit found that there were no documented procedures for all the major activities involved in the management of IT assets. Management has not implemented a lifecycle plan to effectively manage the inventory of IT assets. The audit also found that the process used to track and monitor IT assets had several controls weaknesses, which may result in a loss of assets. Furthermore, the audit found that IMTD does not have a reliable method to track the software installed on CNSC computers and networks.

Overall Recommendation

Management should strengthen its IT asset management processes and systems, in order to meet both the CNSC’s and the Treasury Board’s requirements. The updated processes and systems should address all the recommendations outlined in this report.

Conclusion

The audit concluded that there was a lack of adequate and effective IT asset management processes and controls necessary to maintain the integrity of the IT assets. The audit was unable to determine the completeness and accuracy of the software inventory, as no listing of installed software was available. Improvements are needed, in order to: strengthen the governance structure; document processes and procedures; implement an integrated tracking tool; conduct regular monitoring and verification of assets; ensure that storage areas are secure and can safeguard IT assets.

1. Introduction

1.1. Background

Information technology (IT) plays an important role in CNSC operations and represents an essential component of the organization's strategy to increase productivity and enhance mandated services for the benefit of citizens, businesses and employees.

Due to the growth in activities related to the nuclear sector, the CNSC has recruited a number of highly skilled professionals in the scientific, technical and administrative fields. Over the past four years, in order to meet this expansion in the number of full-time staff members, the CNSC has made several investments in IT hardware and software.

Since these represent attractive and important assets, an independent examination of the accuracy and completeness of the inventory and records was proposed to management. This audit is part of the approved *Risk-Based Audit Plan* for 2011–14.

The Information Management and Technology Directorate (IMTD) develops and implements an IT planning process that is integrated with the CNSC's overall corporate planning process and aligned with the investment planning process. The resulting plan defines CNSC IM/IT directions, strategies, architecture and human resource capacity, and how these work together to achieve CNSC business and government-wide strategic objectives. The *IM/IT Plan* reflects CNSC priorities and outlines planned investments, including any acquired services. The CNSC's *IM/IT Plan* is reviewed annually, and updated as required.

Government of Canada common or shared IT assets and services are used as much as possible at the CNSC, as a way to avoid duplication, when such assets and services are available and appropriate. This strategy is aligned with the CNSC's IT management practices, processes and technology architecture.

IT assets and services are reviewed periodically, to identify opportunities for enhancing efficiency, effectiveness and innovation in collaboration with service providers, service users and other stakeholders.

IMTD's objectives for asset management are to:

- Ensure that IT assets meet program needs as well as operational requirements.
- Ensure value for money in IT assets.
- Ensure that procurement activities stand the test of public scrutiny in matters of prudence and integrity, encourage competition, and reflect fairness in spending of public funds.

1.2. Objective and scope

The objectives of the audit were as follows:

- To determine whether adequate and effective IT asset management processes and controls are in place, in order to maintain the integrity of the IT assets while meeting the CNSC's and the Government of Canada's requirements.
- To provide management with assurance that the IT asset inventory and records are complete and accurate.

The scope of the audit was limited to CNSC's information technology hardware and software inventories, and included IT asset management practices in place as of July 2011. The audit focus was on systems and practices used in the governance, management, control and oversight of IT hardware and software assets.

The audit testing excluded:

- Laptops: An inventory test count for laptops was included in the terms of reference (TOR) for this audit. However, at the time of the audit, IMTD had not completed their inventory count of laptops, and could not provide a final list. The CNSC may decide to have the laptops subjected to a future audit.
- Telecommunication equipment (such as Blackberries and cellular telephones) was not included in the TOR for this audit. The CNSC President requested that an audit of this equipment be conducted. Therefore, the OAE plans to table an audit of mobile telecommunication equipment at the July 2012 Audit Committee meeting.
- For logistical reasons, the inventory audited did not include the regional offices. Furthermore, sufficient audit coverage was obtained by only counting the headquarters region.

The audit fieldwork was conducted between October 4, 2011, and December 22, 2011.

1.3. Analysis of risks and audit criteria

The audit team conducted a risk assessment exercise during the planning phase of the audit. The purpose of the assessment was to identify the potential areas of risk such as governance, acquisition, safeguarding and disposal/surplus of IT assets. As a result of the assessment, the following lines of enquiry and related audit criteria were identified.

Line of Enquiry	Audit Criteria
1. IT management governance structures are in place to provide strategic direction for IT asset management.	The CNSC has a governance structure in place, to ensure IT assets are managed appropriately and in compliance with Government of Canada and CNSC policies.
2. Processes are in place for planning the acquisition of IT assets, as well as the replacement and disposal of IT assets.	The CNSC has processes in place for the planning, acquisition, replacement and disposal of IT assets, which meet applicable policies and directives.
3. Processes and systems are in place to record, track, monitor, and safeguard the IT assets inventory.	The CNSC has processes in place to ensure that IT assets are properly recorded and monitored when purchased, deployed, replaced and disposed of, and that they are properly safeguarded.

1.4. Approach and methodology

The planned approach was to review documentation and interview key employees and managers, in order to identify the risks associated with IT asset management and to assess whether controls are in place to mitigate the risks.

The audit methodology included:

- Conducting interviews with managers and staff.
- Reviewing relevant CNSC and Government of Canada documents (including legislation, regulation, policies, directives, processes and procedures).
- Conducting tests on the accuracy of IMTD's inventory of IT assets.

The audit was conducted within the established parameters of the Treasury Board *Policy on Internal Audit,* as well as the *Auditing Standards* for the *Government of Canada*.

1.5. Statement of assurance

Sufficient and appropriate audit procedures have been conducted, and enough evidence was gathered to support the accuracy of the findings and conclusions in this report and to provide an audit level of assurance. The findings and conclusions are based on a comparison of the conditions, as they existed at the time of the audit, against pre-established audit criteria that were agreed on with management. The findings and conclusion are only applicable to the entity examined and for the scope and time period covered by the audit.

2. Observations and Recommendations

The following observations and recommendations are reported according to the lines of audit enquiry outlined in section 1.4.

2.1. Governance structure

The audit expected to find that the CNSC has a governance structure in place, to ensure that IT assets are managed appropriately and in compliance with the Government of Canada's and CNSC's policies.

Treasury Board policies require departments to have governance structures, mechanisms and resources in place, in order to ensure the continuous and effective management of IT assets. The audit, therefore, expected to find not only information on the responsibilities for managing IT assets, but also on the use of the assets and every user's responsibility to safeguard these assets from potential losses.

The audit found a governance structure in place for IT asset management, as outlined in the CNSC *Management of Information Technology Policy*. Although this policy makes reference to the use of IT assets and the objectives of the program, it lacks key governance components found in the Treasury Board policies.

Standardized processes and procedures facilitate the management of IT assets, and ensure that employees perform their duties in a consistent, standardized manner. Such standardization reduces errors and inconsistencies, and provides a mechanism for continuity of service when new employees are hired.

IMTD staff members indicated that their roles and responsibilities were not clearly defined, communicated or understood by all employees involved in the managing and safeguarding of IT assets.

It was also observed that IMTD employees do not perform similar tasks consistently, since there are no written guidelines. Employees do not receive formal training when assigned to multiple functions relating to the management of IT assets. Our interviews noted that the IT procurement officer was the only one who had received procurement training from Public Works and Government Services Canada.

The audit team expected to find procedures for each phase of IT asset management – from planning to disposal. Procedures were expected to be in place for routine tasks such as receiving assets, labelling assets, information flowing through the inventory system, disposing of assets, as well as for the safeguarding of IT assets.

In the absence of documented processes and procedures, the IMTD will be exposed to the risk of inconsistent practices and controls, which may result in errors and the loss of assets.

Conclusion:

The audit concludes that, although a governance structure has been implemented, there is a general lack of processes, procedures and training, which are necessary to effectively implement the CNSC *Management of Information Technology Policy*.

Recommendation # 1

The IMTD Director General should define, document and communicate roles and responsibilities of staff responsible for IT asset management.

Management Response and Action Plan

IMTD agrees with the recommendation. IMTD has developed a new policy instrument (*IT Asset Management Directive*), along with detailed procedures. These documents summarize the roles and responsibilities of staff involved in asset management. IMTD employees responsible for IT asset management are being trained on the procedures, and the new directive will be communicated to all CNSC staff, once approved.

2.2. Acquisition, replacement and disposal of assets

The audit expected to find that the CNSC has processes in place for planning the acquisition, replacement and disposal of IT assets.

2.2.1. Planning

Planning IT asset acquisitions ensures that end-users have the appropriate tools to support the goals of the organization, and that the funds allocated to these assets are spent with due regard to efficiency and economy. Planning, as indicated in the CNSC *Information Management Policy*, should incorporate a lifecycle approach that allows the CNSC to make risk-informed decisions on when to replace an IT asset. The lifecycle plan should include the planning, acquisition, maintenance and disposal of IT assets over their useful life.

IMTD does not have a documented framework for asset lifecycle management and, as a result, the purchases of IT assets are not always executed in a manner that provides

the opportunity to optimize return on investment. The audit found that a lifecycle approach for IT assets is performed by IMTD; however, this lifecycle plan is not documented. An ad-hoc process is utilized to determine how and when assets are replaced. As there is currently no designated budget for IT assets, purchases are based on the availability of funding at year-end. IMTD management has stated that, to date, there have been sufficient year-end funds to meet the CNSC's IT asset requirements. Purchases of IT assets are also supplemented by divisional operating budgets for specific needs or requirements, when applicable.

Recommendation # 2

The IMTD Director General should develop and communicate a lifecycle plan, to ensure that the division is managing the full lifecycle of IT assets in conformity with the required policies. The plan should include a notional budget set up at the beginning of the year, to address lifecycle management needs. This would provide the basis for funding requests.

Management Response and Action Plan

IMTD agrees with the recommendation. IMTD has developed a lifecycle plan that reflects current requirements for asset replacement, and has also streamlined processes for ongoing lifecycle planning. Funding for the lifecycle plan will be included in the IMTD baseline budget on an ongoing basis. Procurement of assets, in accordance with the plan, will take place on a quarterly basis.

2.2.2. Acquisition

Procurement is the process used to acquire IT material needed to fulfill the CNSC's requirements. The process is jointly managed by IMTD and by the CNSC's Contracting and Administration Division. The contracting component of the process was not part of the scope of this audit, as it is currently the subject of another Office of Audit and Ethics audit on contracting and procurement.

The audit team found that a formal documented process was in place for users requesting IT assets. IMTD has also recently developed a *Procurement of Information Technology Hardware and Software Standard,* to assist users when making a request. The standard defines what IT equipment can be procured and installed on the CNSC's network. The objectives of this standard include:

- Keeping costs in line with corporate needs and budget constraints.
- Ensuring IMTD can support and maintain hardware and software.
- Improving management of depreciating equipment (commonly referred to as "ever-greening").
- Ensuring software licensing agreements are maintained.

This standard was last updated in January 2011, and is accessible to all staff on the CNSC intranet. The Information Management procurement officer was well aware of the standard, and indicated that it is a key part of the request process when assessing the needs of the requester.

The audit found appropriate segregation of duties between the contracting and administration staff (who purchase the IT assets) and the IMTD staff (who receive and distribute assets).

The audit found that the current practice for IT hardware purchases is to make bulk purchases at year-end, with installation of the hardware taking place during the following year. IMTD management has indicated that this method enables the CNSC to gain bulk purchase savings. However, no cost-benefit analysis has been performed by management, which would analyse actual savings from this procurement strategy, when other expenses (such as warehousing and shipping fees) are taken into consideration. While we understand that storage costs may not be significant, management may wish to perform a cost-benefit analysis of bulk purchasing and storage against just-in-time purchasing, so as to determine if this impacts the CNSC's approach and costs of acquiring assets. No formal recommendation has been made for this issue, as management is currently revising its procurement strategy.

2.2.3. Disposal of hardware

The Treasury Board Secretariat Directive on *Disposal of Surplus Material* requires any surplus IT assets to be sent to the Industry Canada "Computers for Schools" program, or to a recognized charitable organization. Surplus IT assets are stored temporarily onsite until the receiving organization is available to pick up the assets.

The audit did not find a formal documented process for declaring IT assets as surplus. The internal practice followed consists in creating a list of surplus items and transmitting that list to the receiving organization.

However, although laptops were excluded from the test count portion of this audit, the audit team observed four laptops set aside for a disposal shipment not documented on the disposal list. The audit also observed that three items on the disposal list marked for delivery were not in the disposal area. Lastly, the audit team was unable to determine whether management exercises appropriate oversight over the disposal process. With the current situation, there is a higher risk of improperly disposing of assets.

Conclusion:

The audit concludes that the processes for the planning, acquisition and disposal of IT assets have significant weaknesses, and should be addressed by management.

Recommendation # 3

The IMTD Director General should formally document the process for declaring an asset as surplus, as well as the disposition process.

Management Response and Action Plan

IMTD agrees with the recommendation. IMTD has developed procedures and forms for asset disposition.

2.3. Management of IT assets

The audit expected to find that the CNSC has processes and systems in place to record, track, monitor, and safeguard the IT assets inventory.

2.3.1. Monitoring and tracking of physical inventory (hardware)

The audit expected that the IT assets would be identified and tracked, and that associated records would be periodically monitored and verified to ensure that assets are recorded accurately. The CNSC has a considerable number of IT assets (not including software licenses). We expected to find information in the asset management systems that included all pertinent information about every asset and its location of use.

2.3.2. System for recording physical inventory

The audit found that several methods are used to record inventory information for hardware and software. At the time of the audit, there were four separate IT asset tracking methods in place, and none were integrated. The audit also noted a legacy system used in tracking the assets. However, due to the lack of reporting capabilities and difficulty of use, the system is supplemented by various manual spreadsheets, duplicating information recorded in the legacy system.

The audit team was informed by IMTD that there was a need for multiple systems, as the legacy system had limited functionality, was cumbersome to use, and could not be integrated with any other system. The legacy system does not have the capability to manipulate fields to produce the type of reports that are useful for employees working with IT assets. Consequently, IMTD relies on the manual spreadsheets for tracking assets, but duplicates its efforts by entering asset information into the legacy system for the disposal process. With spreadsheets, there is no method of tracking the history and movement of the asset, and no method of tracking an asset when it is moved from one spreadsheet to another. Therefore, an asset could be removed accidently (or intentionally) from the spreadsheet without any audit trail in the system.

IMTD currently relies on IT staff to send an email to the inventory technician when IT asset are moved to a new location. There is currently no validation that the information

has been sent to the inventory technician, which increases the risk of having inaccurate data and spreadsheets being out of date.

2.3.3. Monitoring and tracking of software

The audit expected to find routine processes for tracking and reporting the software inventory. Even though a list of purchased software is available, IMTD is unable to produce a reliable list of installed software. Without this list, IMTD is unable to efficiently manage the purchase of software licences. The audit was, therefore, unable to verify the software inventory, since no listing of installed software is available.

Recommendation # 4

The IMTD Director General should implement one tracking tool for hardware and software inventory, which would enable IMTD to efficiently track all IT assets.

Management Response and Action Plan

IMTD agrees with the recommendation. IMTD has merged the two systems currently used for tracking hardware inventory into one tracking tool. IMTD has consolidated its software tracking, and this information is consolidated into two spreadsheets. IMTD will also procure and implement an asset management software solution during the 2012–13 fiscal year, at which time both hardware and software tracking will be merged.

2.3.4. Verification and reconciliation

Good management practices require organizations to track their IT assets, in order to verify their location and condition. The asset tracking systems and the data they contain can provide early warning signs of missing assets, and may assist management in deploying unused inventory. Regular verification of the data against the existing physical assets would alert management about weak controls, and would allow management to identify and correct any issues on a regular basis.

The audit found the following:

- Comparisons or reconciliations between the inventory legacy system and manual spreadsheets, in order to ensure completeness and accuracy of the inventory, are not a regular activity.
- Verification for existence of the physical asset against the inventory system is neither scheduled nor performed regularly. We understand that one IT technician conducts spot-checks, but this practice is not consistent across the division.
- There is no ability to track the history of “who moved an asset” or “who made the changes”.

Recommendation # 5

The IMTD Director General should ensure all IT tracking and monitoring systems are reconciled on a scheduled basis.

Management Response and Action Plan

IMTD agrees with the recommendations.

Recommendation # 5 is no longer required. IMTD no longer uses multiple systems for tracking of IT assets; therefore, a reconciliation is not required.

Recommendation # 6

The IMTD Director General should implement a scheduled verification process, to verify the existence of IT assets.

Management Response and Action Plan

IMTD has implemented a scheduled verification process that will, on an ongoing basis, verify the existence of IT assets. A full verification of assets will take place on an annual basis. The IMTD loaner pool will be verified on a monthly basis.

2.3.5. Physical asset identification

The CNSC uses asset tags for most of its IT assets, to identify the type, location and model of assets that are in service. The asset tag is an important tracking tool that allows for verification and reconciliation of IT assets.

The audit found that:

- There is no policy or directive instructing staff on what items should be tagged, inventoried and tracked.
- Asset tags are not always assigned to new assets immediately when received. Assets can be held in storage areas, for several months, without being identified as CNSC property.
- Asset numbers are not assigned sequentially, thus increasing the difficulty in identifying a missing asset.

- There are four different types of asset tags currently being used by IMTD. Some of the tags clearly identified the property as belonging to CNSC, while others did not.

- Unsecured asset tags were found in the technical rooms; they were accessible to all IMTD employees.

There is a risk that IT asset purchases are not properly recorded, and that assets could be misappropriated.

Recommendation # 7

The IMTD Director General should implement a documented process for assigning asset numbers to IT assets.

Management Response and Action Plan

IMTD agrees with the recommendation. IMTD has implemented a documented process for assigning asset numbers to IT assets.

2.3.6. Safeguarding assets

In order to safeguard IT assets, controls should be in place to secure them from theft or misuse.

The audit found that when new IT assets are received, they are sent to the mailroom for pick-up by IMTD staff, without immediate inspection. At times, assets arrive broken during shipment from the supplier, and the CNSC assumes ownership of the asset regardless of its condition, upon receipt at the front desk. Management might wish to add additional controls with regards to the receipt of IT equipment, as well as a number of quality steps; the CNSC should return the equipment, if it is not in an acceptable condition at receipt.

New assets are then brought to a designated area, unpacked and stored temporarily. This area can be accessed by all CNSC staff, and the audit observed that the door to the area is frequently left open by technicians. Furthermore – according to the IMTD employees, and as observed by the audit – the Slater street technician room that contains assets is left unlocked when employees are not present. Finally, we also observed untagged assets on the floor of the room.

Recommendation # 8

The IMTD Director General should ensure that all IT assets are secured. Management should separate the storage of new IT assets from IT assets that are designated for disposal.

Management Response and Action Plan

IMTD agrees with the recommendation. IMTD has reviewed physical space layout and developed procedures, in order to ensure that IT assets are secured, and that the storage of new IT assets is separated from the storage of IT assets that are designated for disposal.

2.3.7. Storage of IT assets

IMTD keeps a supply of IT assets on hand, to ensure continuity of service for end-users. Since the physical space at CNSC headquarters is limited, inventories of new assets are warehoused offsite, and some are stored onsite in a designated secured storage area.

- **Offsite warehousing**

  The auditors performed a count verification of IT assets at the offsite warehouse, and found that all assets were accounted for. We noted that some high value assets had been in storage for more than a year.

- **Onsite storage**

  The audit found the onsite storage area contained both new IT assets (not yet deployed) and used IT assets (scheduled to be disposed). We found high-dollar value assets that neither had asset tags nor were on IMTD's inventory list. This issue was also discussed in section 2.3.5

Recommendation # 8 applies to section 2.3.7 as well.

Conclusion:

The audit concludes that the processes and systems to record, track, monitor and safeguard the IT assets either have significant weaknesses, or do not exist at all; this should be addressed immediately by management.

3. Inventory Testing

In the fall of 2011, IMTD performed a complete count of all physical IT assets owned by the CNSC. The inventory count was to confirm the presence and location of the physical inventory. The inventoried IT assets included network infrastructure equipment, desktop computing equipment, printing equipment and peripherals (used in conjunction with the desktops).

The audit performed a physical count of all IT assets located at the Telesat and Slater buildings, as well as in various storage areas within the Ottawa area, based on the listing supplied by IMTD as at December 6, 2011. Due to the weaknesses identified in the processes and procedures in the management of IT assets, the audit team did not

perform any testing on whether purchases were properly recorded in inventory listings. Instead, the auditors performed a count to confirm the existence of the assets. The CNSC may decide to have an audit of IT purchases performed at a later date.

In total, the audit counted 5,464 pieces of IT assets (hardware). The audit did not find significant variances between the physical count and inventory listing. Some of the significant results of our count are as follows:

- 13 IT assets had asset tags, but were not on the inventory list.
- 41 audio-visual equipment items had tags, but were not on the inventory list.
- 12 IT assets on the inventory list could not be located.
- Six IT assets were found by the audit, but did not have an asset tag.
- Several IT assets that were recently installed (according to the users) were neither tagged, nor on the inventory list.
- Several IT assets listed on the inventory list had the incorrect asset tag numbers.

Audio-visual equipment was not included in the scope of the audit. However, since some of this equipment is connected to the CNSC network, the audit team decided to include these particular items in the audit. The following weaknesses specifically related to audio-visual equipment were observed during the count:

- Even though audio-visual equipment is under the responsibility of IMTD, they have the equipment only partially inventoried.
- The audit team found that audio-visual equipment was not consistently listed in the IT asset inventory.
- Audio-visual equipment was found to be inconsistently tagged.

The audit team realises that the discrepancies outlined above are not material. However, as noted in previous sections of the report, controls need to be further strengthened, to account and report on IT assets.

Conclusion:

The audit concludes that most of the assets in the inventory reported by IMTD were present and at the location identified by IMTD. The audit further concludes that the inventory listing is neither complete nor accurate.

Recommendation # 9

The IMTD Director General should develop and implement a process to track the location of the audio video equipment using the asset numbers assigned to this equipment.

Management Response and Action Plan

IMTD agrees with the recommendation. IMTD has developed and implemented procedures to ensure that audio-video equipment is tracked using assigned asset numbers.

4. Overall Recommendation

Management should develop and implement an IT asset management system that would meet both the CNSC's and the Treasury Board's requirements. That system should address all the recommendations outlined in this report.

5. Overall Conclusion

The audit concluded that there was a lack of adequate and effective IT asset management processes and controls to maintain the integrity of the IT assets. The audit was unable to determine the completeness and accuracy of the software inventory, as no listing of installed software was available. As a result, the CNSC may be at risk – legally and financially – of operating unlicensed software. Improvements are needed to strengthen the governance structure, document the processes and procedures, implement an integrated tracking tool (along with regular monitoring and verification), and to ensure storage areas are appropriate to safeguard IT assets.

Upon a review of this audit report, the Audit Committee requests the Office of Audit and Ethics to perform a follow-up audit to the recommendations found in this document, and provide their conclusions at the November 2012 Audit Committee meeting.

Appendix A – Detailed Audit Criteria

Criteria	Sub-Criteria
1. The CNSC has a governance structure in place, to ensure that IT assets are managed appropriately and in compliance with Government of Canada and CNSC policies.	**1.1** - There is an IT assets management structure in place that defines accountability for IT assets.
	1.2 - Roles and responsibilities are clearly defined and communicated.
	1.3 - Employees responsible for IT asset management are provided with training.
2. The CNSC has processes in place for the planning and acquisition of IT assets, as well as the replacement and disposal of IT assets, which meet the applicable policies and directives.	**2.1** - The CNSC has a plan for the acquisition/replacement and disposal of IT assets.
	2.2 - There are processes and procedures in place for the planning/purchase/replacement and disposal of IT assets.
	2.3 - IMTD and Contracting & Procurement comply with the CNSC and Treasury Board policies for the purchase/disposal of IT assets.
	2.4 - A hardware and software standard is developed and implemented.
	2.5 - The CNSC mitigates the risk of employees benefitting from the purchase of IT assets.
3. The CNSC has processes in place to ensure that IT assets are recorded, tracked and updated when purchased, deployed, replaced or disposed of, and that they are properly safeguarded.	**3.1** - An asset tracking system is in place for IT asset inventory management, including software licensing.
	3.2 - IT assets are assigned asset numbers for tracking purposes.
	3.3 - The tracking system is kept up to date with all IT assets.
	3.4 - IT assets and records are periodically verified, to ensure assets have not gone missing.
	3.5 - IT assets are stored properly, in a locked area, when not in use.
	3.6 - CNSC keeps a record of IT assets that have been disposed of or deemed surplus, as per TBS directive on disposal of surplus materiel.
	3.7 - CNSC has software licenses for applications in use.

Appendix B – Overview of Audit Recommendations and Management Response and Action Plans (MAP)

1. Recommendation: The IMTD Director General should define, document and communicate roles and responsibilities of staff responsible for IT asset management.		
Unit Responsible	Management Response	Timeline
IMTD	Agreed. IMTD has developed a new policy instrument (*IT Asset Management Directive*), along with detailed procedures. These documents summarize the roles and responsibilities of staff involved in asset management. IMTD employees responsible for IT asset management are being trained on the procedures, and the new directive will be communicated to all CNSC staff once approved.	Directive – **Completed** (in final approvals) Procedures – **Completed**
2. Recommendation: The IMTD Director General should develop and communicate a lifecycle plan, to ensure that the division is managing the full lifecycle of IT assets, in conformity with the required policies.		
Unit Responsible	Management Response	Timeline
IMTD	Agreed. IMTD has developed a lifecycle plan that reflects current requirements for asset replacement, and has also streamlined processes for ongoing lifecycle planning. Funding for the lifecycle plan will be included in the IMTD baseline budget on an ongoing basis. Procurement of assets, in accordance with the plan, will take place on a quarterly basis.	**Completed** (ongoing activity)
3. Recommendation: The IMTD Director General should formally document the process for declaring an asset as surplus, as well as the disposition process.		
Unit Responsible	Management Response	Timeline
IMTD	Agreed. IMTD has developed procedures and forms for asset disposition	**Completed**

4. Recommendation: The IMTD Director General should implement one tracking tool for hardware and software inventory, which would enable IMTD to efficiently track all IT assets.		
Unit Responsible	Management Response	Timeline
IMTD	Agreed. IMTD has merged the two systems currently used for tracking hardware inventory into one tracking tool. IMTD has consolidated its software tracking, and this information is consolidated into two spreadsheets. IMTD will also procure and implement an asset management software solution during the 2012–13 fiscal year, at which time both hardware and software tracking will be merged.	Merging of two hardware tracking tools – **Completed** as of February 8, 2012. Software tracking has been consolidated and merged into two spreadsheets, as of May 1, 2012. Asset management solution implementation: requirements and options analysis underway.
5. Recommendation: The IMTD Director General should ensure all IT tracking and monitoring systems are reconciled on a scheduled basis.		
Unit Responsible	Management Response	Timeline
IMTD	Recommendation # 5 is no longer required. IMTD no longer uses multiple systems for tracking of IT assets; therefore, a reconciliation is not required.	N/A
6. Recommendation: The IMTD Director General should implement a scheduled verification process, to verify the existence of IT assets.		
Unit Responsible	Management Response	Timeline
IMTD	Agreed. IMTD has implemented a scheduled verification process that will, on an ongoing basis, verify the existence of IT assets. A full verification of assets will take place on an annual basis. The IMTD loaner pool will be verified on a monthly basis.	**Completed** (ongoing activity)

7. Recommendation: The IMTD Director General should implement a documented process for assigning asset numbers to IT assets.		
Unit Responsible	Management Response	Timeline
IMTD	Agreed. IMTD has implemented a documented process for assigning asset numbers to IT assets.	**Completed**
8. Recommendation: The IMTD Director General should ensure that all IT assets are secured. Management should separate the storage of new IT assets from IT assets that are designated for disposal.		
Unit Responsible	Management Response	Timeline
IMTD	Agreed. IMTD has reviewed physical space layout and developed procedures, in order to ensure that IT assets are secured, and that the storage of new IT assets is separated from the storage of IT assets designated for disposal.	**Completed**
9. Recommendation: The Director General, IMTD should develop and implement a process to track the location of audio-video equipment, using the asset numbers assigned to this equipment.		
Unit Responsible	Management Response	Timeline
IMTD	Agreed. IMTD has developed and implemented procedures to ensure that audio-video equipment is tracked using assigned asset numbers.	**Completed**