Fisheries and Oceans Canada | Pêches et Océans Canada

Internal Audit Report

Audit of Information Technology Asset Management

Project 6B302

Date: June 2019

Canada

Table of Contents

Introduction

This internal audit engagement was requested by the Information Management and Technology Services Directorate and conducted in accordance with Fisheries and Oceans Canada's Internal Audit Directorate's (IAD) Risk-Based Audit Plan 2018-2020.

Asset and Lifecycle management (ALCM) of Information Technology (IT) involves tracking of IT assets throughout their life from purchase through disposal to ensure more informed and timely purchasing and replacement, better understanding of total cost of ownership and disposals that are in line with government priorities.

The Department currently tracks its IT assets with two tools: Microsoft System Centre Configuration Manager (SCCM); and Axios Assyst. As of November 2018, SCCM indicated that the Department has 3522 desktops, 7581 laptops, 1015 power PCs, and 524 tablets on the Department's network. Further, the Department spends on average $5 million each year on purchasing IT hardware.

At Fisheries and Oceans Canada (DFO), the main responsibility for IT asset management falls to the ALCM Team within the Information Management and Technology Services Directorate (IMTS). In addition to the ALCM Team, the Service Desk within IMTS carries out replacements for IT assets that are damaged, broken, lost or stolen, and deployments for new employees. Similarly, the Business Management, Integration and Engagement group within IMTS does procurement of all IT assets.

Why this audit is important

Information Technology plays a vital role within the Government of Canada by supporting efficient service delivery, enabling communication, encouraging openness and transparency, and increasing the accessibility of programs and services to Canadians. Informed decisions about IT asset investments, costs, and risks are essential to successful government plans and priorities.

Sound IT asset management practices are needed to manage the lifecycle of IT assets from purchase to end of life. Not only is IT asset management important to reduce costs, improve operational efficiency, determine the full cost of existing investments and provide accurate cost information to guide future investment decisions, but it can also help identify and manage information risk and security issues across the network. Lifecycle management, a best practice in IT asset management, involves maintaining an accurate inventory of IT assets and ensuring each phase from planning to disposal is done in a manner that optimizes performance, usefulness and value-for-money.

Information Technology is a strategic asset and key enabler of DFO's program mandate and goals. According to the 2018-21 DFO Information Management and Information Technology Plan, the Department is developing and implementing a modern IT infrastructure that enables effective, efficient and timely availability of information and ensures the safeguarding of departmental information assets. This audit seeks to help inform Departmental decision makers as they look to develop and implement this infrastructure.

Audit Objective

The purpose of this audit is to determine whether Fisheries and Oceans Canada has in place an effective IT asset management system for hardware devices that protects these assets and information, complies with regulations, and supports program delivery.

Audit Scope

The audit examined the controls, including procedures and guidance, over IT asset management of hardware devices within the Department, as well as the processes and practices for the disposal of these IT assets. The audit focused specifically on hardware devices, including, but not limited to, desktops, laptops, monitors, tablets, and printers.

The audit did not examine the following aspects of IT assets and their management:

- Software, as it was recently subject to an internal review;
- Cell phones, smartphones and servers, as these are managed by Shared Services Canada; and
- Specialized IT assets designed for use by the Canadian Coast Guard and specialized scientific equipment, as these items are not purchased through or managed by IMTS.

This was not an audit of any security controls outlined in the TBS Policy on Government Security.

Audit Approach

The audit team carried out its mandate in accordance with the Treasury Board *Policy on Internal Audit* and *Directive on Internal Audit,* as well as the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing. The audit employed various techniques including a risk assessment of the audit entity, interviews, site visits, as well as review and analysis of documentation and information.

Audit Findings

Internal Controls

Accuracy and Completeness of IT Hardware Asset Inventories

Having an accurate and up-to-date inventory of IT hardware assets is necessary for effective lifecycle management, protection of assets from loss, accurate planning and budgeting and ease of locating assets when needed. In the absence of an accurate and up-to-date inventory, the Department is at risk of not having critical IT assets available when needed. To test the accuracy of the existing inventories of IT hardware assets, interviews were carried out and samples from each of the Assyst, Abacus and Printer Inventories were taken, along with substantive testing of the Primary Distribution Center and two of the three Secondary Distribution Center Inventories. In discussing these inventories, interviewees were consistent in stating that none of them was accurate nor up-to-date. This was confirmed through testing which is summarized below by inventory.

The Axios Assyst Inventory includes all types of laptops, desktops, and tablets. Further, monitors have been added within the last year. While this inventory is maintained primarily by the ALCM team within IMTS, the IT Service Desk is responsible for the monitors portion and updating inventory that they deploy. To test the accuracy of this inventory, a February 2019 extract from Axios Assyst was obtained for all types of laptops, desktops and tablets listed as deployed and all monitors listed as shipped and available. The monitors listing included 864 monitors from which a sample of 38 was selected. None of the 38 monitors were found in the location identified in the inventory. The deployed inventory, consisting of all types of laptops, desktops and tablets amounted to 13,257 assets, from which a sample of 281 assets was selected for testing. Overall 113, or 40%, of the assets were found to be accurate (in the possession of the person indicated, in the region indicated). The remaining 168, or 60%, were either not found or were not with the person or location listed. While this includes both judgemental and

random samples, accuracy only increases to 46% when only the random samples are considered. These results are consistent with preliminary testing done in the planning phase. Also, analysis of the Assyst Inventory listing showed that there were 337 deployed assets without any assigned user and 18% were not assigned to a cost center. Finally, Assyst also includes 9,514 IT assets that are currently listed as "surplus".

The Abacus Inventory is the inventory within the Department's Financial System. While a decision was made four years ago not to record any IT assets under $10,000 in the assets listing within Abacus, the inventory had 3,892 active assets coded to IT hardware in October 2018. To test the accuracy of this inventory, a sample of 68 IT assets were selected, none of which were found in the locations indicated. Additional analysis of the Abacus inventory showed that it includes: 2,254 printers, of which 88% are over 10 years old with the oldest dating back to 1985; 382 servers, 97% of which are over 10 years old and servers are now managed by Shared Services Canada; and 422 scanners, of which 85% are over 10 years old. Finally, a number of items were found to be incorrectly coded to IT hardware, including a kayak, a model boat and artwork.

The Printer inventory is an Excel spreadsheet that lists printers purchased or leased since December 2015. A sample of 10 printers from this listing was selected, 7 were found to be accurate, while the remaining 3 were not found in the location indicated in the inventory.

Finally, the Primary and Secondary Distribution Center's tracking sheet is an Excel Spreadsheet that is maintained to identify current inventory levels of desktops, laptops, power PCs and tablets. Substantive testing of the Primary Distribution Center's tracking records showed they were accurate, except for 12 tablets found on location that were not listed in the inventory. The two Secondary Distribution Centers tested did not have accurate inventory records.

While these inventory errors were found to be significant, they could be improved through the implementation of key controls, including limiting access to who can input and change information in the inventories, having mandatory updating of inventory information, and putting in place automated controls to limit input and removal errors.

Recommendation 1: The Assistant Deputy Minister (ADM) of Human Resources and Corporate Services (HRCS) should implement key controls, including limiting access to who can change information in asset inventories, mandatory updating, and putting in place controls to limit input and removal errors. The ADM should also determine the practicality of establishing a single inventory covering a reasonable time period. If practical, such a single inventory should be put in place.

Management Response:
Management Agrees with the recommendation
The ADM of HRCS will work with Chief Information Officer (CIO), Desktop Engineering and Asset Management (DEAM), Information Technology Service Desk (ITSD) and Information Technology Service Management (ITSM) to:

- Review inventory tools, including but not limited to Assyst 11 with the objective of recommending a tool that provides automated controls;
- Review access permissions, and limit access to the Configuration Management Database (CMDB) where possible;
- Review and add DFO owned printers in the database instead of using spreadsheets;
- Incorporate the distribution centers spreadsheet information into the Assyst database;

- Prepare action plan for refreshing current inventory;
- Conduct refresh of inventory;
- Review and communicate strategies (Responsible-Accountable-Consulted-Informed(RACI) Model and Processes) to the limited staff that are part of delivering the updated inventory; and
- Setup a quarterly quality assurance audit on all staff and processes to make sure system stays accurate in the long term.

Planned completion date: March 31, 2021

Recommendation 2: The CFO should review and update all IT Hardware Assets listed in Abacus.

Management Response:
Management Agrees with the recommendation
The CFO will review the list of IT Assets in Abacus and retire categories of items tracked in other systems by IMTS and correct coding for the remaining assets.
Planned completion date: September 30, 2019

Processes and Controls for IT Asset Hardware Management

Processes that are supported by risk-based controls help ensure that management of IT assets can be carried out effectively and efficiently while also protecting those assets from loss. Without consistent and effective processes in place, it is difficult to ensure the adequacy and accuracy of the IT asset inventory or that the assets support program delivery. To test for effective processes and controls, interviews, walk-throughs and a review of documents took place. The information found in these activities was then used to prepare process flowcharts for review and comparison against best practices. Analysis of these processes and controls showed that they are often reactive rather than proactive and are sometimes created in silos, resulting in weaknesses related to protection of assets, the resourcing model and coordination of asset management.

Protection of Assets

Protection of IT assets is not only important to prevent loss of physical assets but also to ensure information contained on those assets is not inadvertently disclosed. Weaknesses in asset protection were found at each phase of the asset lifecycle.

In the asset acquisition phase, controls that would ensure items purchased were recorded in the inventory were missing. Currently, the responsibility of ensuring that laptops, desktops and tablets are received, requested to be entered into the system and distributed, falls to one person without any further verification or automated controls.

Once the assets are in the inventory, the Department uses Axios Assyst to track most of its IT hardware assets. Currently, employees with access to the asset module within Assyst are able to make changes to an asset's status without restrictions or automated controls. As a result, an employee with access to both the asset and the asset module in Assyst, can change the status of the asset and remove it from the Department with minimal risk of detection. Further, one of the main controls in the system is to have users voluntarily type in changes and explanations into a "movement field". There are 334 employees in the Department who have access to the assets module in Assyst, as well as 4 administrative accounts with no controls over entry, changes or deletions. One impact of this was seen in a sample of 79 disposals, where four assets with a status of disposed of, discontinued or surplus were found to be still

in use. Similarly, once assets have been distributed to end users, the Department uses SCCM software to identify which assets are logged into the system; however, no reconciliation of the data in SCCM and the Asset Inventory listing is done.

Finally, on site visits, assets were often found in unsecured locations. This included new assets as well as surplus used equipment, including desktops.

Recommendation 3: The ADM of HRCS should review the IT asset management process to ensure that controls are in place to protect assets.

Management Response:
Management Agrees with the recommendation
The ADM of HRCS in collaboration with the CIO, Real Property, Safety and Security (RPSS), DEAM, ITSD and ITSM will:

- Review, update when required, and communicate current ITSM processes related to protection of assets;
- Review access permissions and remediate as per requirements; and
- Review current conditions at primary and secondary distribution centers and ITSD sites to improve security posture.

Planned completion date: March 31, 2021

Resourcing Model

Lifecycle management involves replacing assets at an optimal age to minimize asset failures while maximizing use. These scheduled replacements reduce disruptions to operations, preserves data stored on the asset and reduce time and data loses due to asset failures. While IMTS has plans to replace assets at an optimal asset age, the current funding model requires that they obtain funds from sectors to be able to do so. As a result, the ALCM team has not been able to replace all assets within the assets useful life. Currently, 34.4% of the deployed assets in Assyst have exceeded their useful life. This can result in increased asset failures which can disrupt operational activities. Further, while sectors are more likely to have funds available for asset replacements at year-end, these funds are not always able to be used due to procurement deadlines.

Not replacing assets within their useful life also impacts planned IT projects such as the Department's current initiative to upgrade to Windows 10. Assets that exceeded their useful life were not all able to be upgraded to Windows 10 resulting in ALCM having to urgently replace computers for this project out of an already limited stock, adding time needed to complete the upgrade. Also, without an effective resourcing model, there is increased risk of not having adequate inventory on hand for urgent needs such as replacing assets that have failed or providing assets to new employees. This can result in disruption to program delivery as the mandatory processes for procuring IT assets are not conducive to obtaining assets quickly.

Recommendation 4: The ADM of HRCS, in consultation with the CFO, should consider alternative funding models for IT Asset lifecycle management to ensure assets can be managed effectively, including scheduled replacements.

Management Response:
Management Agrees with the recommendation

The ADM of HRCS, in consultation with CFO and in collaboration with CIO, DEAM and the BMIE finance team will:

- Review the current funding model and its ability/inability to sustain a healthy Asset Lifecycle Management (ALCM) for DFO; and
- Propose an alternative funding model that is reflective of today's IT Asset landscape and requirements.

Planned completion date: December 31, 2019

Coordination

Coordination of the management of IT assets involves ensuring that all those involved in the process are aware of their roles and responsibilities. Currently, sectors or users are not actively involved in verifying the accuracy of the IT assets assigned to them which impacts the inventory accuracy. Also, while there is a form in Axios Assyst to report the transfer of an IT Asset to another user, the associated $500 fee, and lack of awareness among sectors of the importance of reporting these transfers, results in transfers not being consistently reported.

Recommendation 5: The ADM of HRCS should ensure coordination between IMTS and sectors with clear accountabilities, roles and responsibilities, and an annual verification of IT hardware assets.

Management Response:
Management Agrees with the recommendation
The ADM of HRCS will work with Regional Director Generals, CIO, Client Portfolio Management (CPM) and DEAM to create a clear asset management process, including Quality Assurance (QA), and Responsible-Accountable-Consulted-Informed (RACI).
Planned completion date: March 31, 2020

IT Hardware Asset Disposals

Ensuring assets are disposed of as effectively as possible, as soon as possible after they become surplus and in compliance with regulations helps ensure the Department is meeting data protection requirements and government stewardship priorities while reducing costs related to storing assets and maximizing the potential for reuse of those assets. Based on interviews, there is a lack of consistent understanding of the process for disposal or what documentation and coordination is required. This was confirmed in a sample of 79 disposals (59 from Assyst and 20 from Abacus) of which 42, or 53%, had no supporting documentation.

Further, based on interviews and site visits, assets are not being disposed of as soon as possible after they become surplus, as required. Specifically, assets are not consistently returned by clients for disposal. This is supported by site visits which found IT hardware assets not being used, some for several years. It is also consistent with analysis of the Assyst records which showed that there were 772 assets marked as "to be returned". Finally, one region mentioned that they had over 3,000 hard drives in storage waiting for destruction with some having been there as long as 15 years.

For the IT Hardware Disposal Process, there are three major regulation requirements:

1) That all information and assets are protected from loss, theft, or misuse.
2) That auditable records of the costing analyses that were used to justify disposal decisions are maintained.

3) That Computers for Schools (CFS) be offered right of first refusal for all surplus IT Hardware Assets.

Opportunities for improvement in the protection of assets from loss, theft, or misuse were found. Specifically, there is a lack of controls within Assyst to require additional verification or approval when an asset still within its useful life is classified as surplus, e-waste, CFS or discontinued. Of the 59 Assyst disposals examined, eight were less than one year old at the time of disposal and six of those had no explanation as to why they were being disposed of. Also, none of the disposals tested included analysis of the security level of information contained on the device and only 9, or 11% had evidence of the asset being wiped or the hard drive removed before disposal. Finally, it was found that listings from Computers for Schools or Ewaste were not being reconciled with disposal records making it difficult to ensure assets were disposed of via the means indicated.

Similarly, none of the items in the selected disposals included costing analysis to justify the disposal decisions. Finally, only one of the 79 disposal samples examined had evidence that it had been offered to Computers for Schools first.

Recommendation 6: The ADM of HRCS should ensure that clear disposal processes and controls are put in place to ensure compliance with mandatory regulations and the protection of assets.

Management Response:
Management Agrees with the recommendation
The ADM of HRCS, in collaboration with the CIO, DEAM, ITSD and Material Management will:

- Review the current processes related to disposal of assets and ensure compliance with the following regulations:
    - that all information and assets are protected from loss, theft or misuse;
    - that auditable records of the costing analyses that were used to justify disposal decisions are maintained; and
    - that Computers for Schools (CFS) be offered right of first refusal for all surplus IT Hardware Assets.
- Implement a process to effectively destroy damaged/expired hard drives that represent a risk of data exposure.

Planned completion date: March 31, 2020

Conclusion

Fisheries and Oceans Canada does not have in place an effective IT asset management system for hardware devices that protects these assets and information, complies with regulations, and supports program delivery.

Opportunities for improvement were identified to strengthen the inventory of IT hardware assets, the protection of IT assets, the resourcing model for ALCM, the coordination of IT asset management and the disposal of IT assets.

Statement of Conformance

In my professional judgment as Chief Audit Executive, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the opinion provided and contained in this report. The extent of the examination was planned to provide a reasonable level of assurance

with respect to the audit criteria. The 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. The opinion is applicable only to the entity examined and within the scope described herein. The evidence was gathered in compliance with the Treasury Board Policy and Directive on Internal Audit. The audit conforms with the Internal Auditing Standards for the Government of Canada, as supported by the results of the Quality Assurance and Improvement Program (QAIP). The procedures used meet the professional standards of the Institute of Internal Auditors. The evidence gathered was sufficient to provide Senior Management with proof of the opinion derived from the internal audit.

Appendix A: Lines of Enquiry and Audit Criteria

The audit criteria are presented in the table below, by audit line of enquiry.

Audit Criteria
Line of Enquiry 1 – Controls
Criterion 1.1: The Department maintains an accurate and up-to-date inventory of its IT hardware assets.
Criterion 1.2: The Department has IT asset management processes and controls in place that support effective and efficient program delivery and protection of its assets.
Line of Enquiry 2 – Compliance
Criterion 2.1: The Department disposes of its IT hardware assets as effectively as possible, as soon as possible after they become surplus to the requirements of program delivery, and in compliance with regulations.

Appendix B: Recommendations and Management Responses

Recommendation	Management Response
The Assistant Deputy Minister (ADM) of Human Resources and Corporate Services (HRCS) should implement key controls, including limiting access to who can change information in asset inventories, mandatory updating, and putting in place controls to limit input and removal errors. The ADM should also determine the practicality of establishing a single inventory covering a reasonable time period. If practical, such a single inventory should be put in place.	*Management Agrees with the recommendation.* The ADM of HRCS will work with Chief Information Officer (CIO), Desktop Engineering and Asset Management (DEAM), Information Technology Service Desk (ITSD) and Information Technology Service Management (ITSM) to: • Review inventory tools, including but not limited to Assyst 11 with the objective of recommending a tool that provides automated controls; • Review access permissions, and limit access to the Configuration Management Database (CMDB) where possible; • Review and add DFO owned printers in the database instead of using spreadsheets; • Incorporate the distribution centers spreadsheet information into the Assyst database; • Prepare action plan for refreshing current inventory; • Conduct refresh of inventory; • Review and communicate strategies (Responsible-Accountable-Consulted-Informed(RACI) Model and Processes) to the limited staff that are part of delivering the updated inventory; and • Setup a quarterly quality assurance audit on all staff and processes to make sure system stays accurate in the long term. **Planned completion date:** March 31, 2021
The CFO should review and update all IT Hardware Assets listed in Abacus.	*Management Agrees with the recommendation.* The CFO will review the list of IT Assets in Abacus and retire categories of items tracked in other systems by IMTS and correct coding for the remaining assets. **Planned completion date:** September 30, 2019

The ADM of HRCS should review the IT asset management process to ensure that controls are in place to protect assets.	*Management Agrees with the recommendation.* The ADM of HRCS in collaboration with the CIO, Real Property, Safety and Security (RPSS), DEAM, ITSD and ITSM will: • Review, update when required, and communicate current ITSM processes related to protection of assets; • Review access permissions and remediate as per requirements; and • Review current conditions at primary and secondary distribution centers and ITSD sites to improve security posture. **Planned completion date:** March 31, 2021
The ADM of HRCS, in consultation with the CFO, should consider alternative funding models for IT Asset lifecycle management to ensure assets can be managed effectively, including scheduled replacements.	*Management Agrees with the recommendation.* The ADM of HRCS, in consultation with CFO and in collaboration with CIO, DEAM and the BMIE finance team will: • Review the current funding model and its ability/inability to sustain a healthy Asset Lifecycle Management (ALCM) for DFO; and • Propose an alternative funding model that is reflective of today's IT Asset landscape and requirements. **Planned completion date:** December 31, 2019
The ADM of HRCS should ensure coordination between IMTS and sectors with clear accountabilities, roles and responsibilities, and an annual verification of IT hardware assets.	*Management Agrees with the recommendation.* The ADM of HRCS will work with Regional Director Generals, CIO, Client Portfolio Management (CPM) and DEAM to create a clear asset management process, including Quality Assurance (QA), and Responsible-Accountable-Consulted-Informed (RACI). **Planned completion date:** March 31, 2020

The ADM of HRCS should ensure that clear disposal processes and controls are put in place to ensure compliance with mandatory regulations and the protection of assets.	*Management Agrees with the recommendation.*
	
	The ADM of HRCS, in collaboration with the CIO, DEAM, ITSD and Material Management will:
	• Review the current processes related to disposal of assets and ensure compliance with the following regulations:
	  ○ that all information and assets are protected from loss, theft or misuse;
	  ○ that auditable records of the costing analyses that were used to justify disposal decisions are maintained; and
	  ○ that Computers for Schools (CFS) be offered right of first refusal for all surplus IT Hardware Assets.
	• Implement a process to effectively destroy damaged/expired hard drives that represent a risk of data exposure.
	Planned completion date: March 31, 2020