Health Canada and the Public
Health Agency of Canada

Santé Canada et l'Agence
de la santé publique du Canada

Audit of Information Technology Asset Management at Health Canada and the Public Health Agency of Canada

Draft Report presented to the Health Canada and the Public Health Agency of Canada Departmental Audit Committees

January 18, 2022

Table of Contents

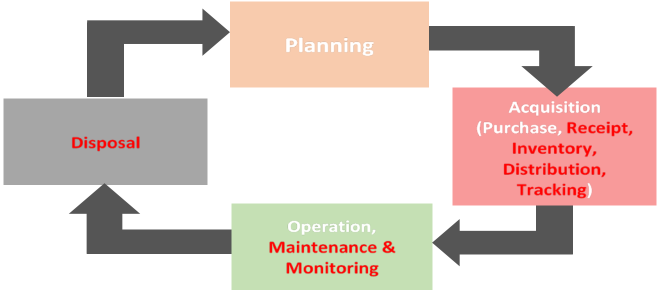
List of Acronyms

Acronym	Title
ACAR	Annual Capital Asset Review
AIVE	Asset Inventory Verification Exercise
CFOB	Chief Financial Officer Branch
EAM	Entreprise Asset Management (solution)
HC	Health Canada
IMSD	Information Management Services Division
IT	Information Technology
ITAM	Information Technology Asset Management
MAMD	Material and Asset Management Division
NML	National Microbiology Laboratory
PHAC	Public Health Agency of Canada
SAM	Software Asset Management
SAP	Systems Applications and Products
TBS	Treasury Board Secretariat

Executive Summary

What we examined

Information Technology Asset Management (ITAM) is the process by which Information Technology (IT) assets are managed throughout their lifecycle.


Planning
Acquisition (Purchase, Receipt, Inventory, Distribution, Tracking)
Operation, Maintenance & Monitoring
Disposal

The audit lines of enquiry and the audit criteria focused on those areas of the IT asset lifecycle highlighted in red above:

- Inventory Management (receipt, inventory, distribution) and Tracking
- Monitoring and Maintenance
- Disposal

The audit findings, conclusions and recommendations are presented in the report along these three lines of enquiry and their related audit criteria.

What we expected

For the purposes of this audit, we defined IT assets to be hardware, such as laptops, tablets, servers, and monitors; general desktop software, such as word processing and communication programs;, and business applications, which are systems that are used directly by end users to support specific core business processes.

The three systems supporting the management of IT assets relevant to the audit scope are: Systems Applications and Products (SAP), the financial system of record for HC and PHAC; Application Portfolio Management (APM) Core, the database that tracks applications, including business applications; and the Software Asset Management (SAM) Database.

Below is a high-level description of how the lines of enquiry, asset type, and supporting systems interrelate.

	Inventory Management and Tracking	Monitoring and Maintenance	Disposal
Hardware Assets	SAP	SAP	SAP
Software Assets	SAP and SAM Database	SAP and SAM Database	SAP
Business Applications	APM Core	APM Core	APM Core

We examined the controls, processes, and systems in place to ensure appropriate management of IT assets, as governed by the Treasury Board (TB) *Policy Framework for the Management of Assets and Acquired Services,* the TB *Policy on Management of Materiel*, as well as the Health Canada (HC) and the Public Health Agency of Canada (PHAC) Standard on Asset Management and ITAM Guide from 2015-16 to 2019-20.

Within HC and PHAC, the stakeholders involved in the areas of IT asset management that are in scope for this audit are: the Information Management Services Division (IMSD), the Material Asset Management Division (MAMD), the Application Portfolio Management (APM) group (IMSD), various Laboratories within HC, and HC and PHAC cost centre managers (CCMs).

Why it's important

All employees and programs rely on IT assets, including hardware, software, and business applications, to conduct their daily work and meet program objectives. Both the Department and Agency have complex science-based digital environments, and it is vital that IT assets are managed in a manner that maximizes their availability and reliability to stakeholders. In enabling the delivery of programs and services, it is also important to effectively manage the scarce resources available for maintaining the health of the IT assets, to derive more value from the assets in terms of use and efficiency, and to secure the data residing within the IT assets.

What was found

Overall, while we noted some positive aspects of the management of IT hardware assets and business applications, we found incomplete and inaccurate data in each of the IT asset supporting systems, along with inadequate governance and support for planning and engagement for IT asset management. These gaps have impeded HC and PHAC's ability to make fully informed decisions about asset investment, maintenance, and disposal, as well as impeding their focus on prioritizing and fulfilling asset initiatives in a cost-effective, proactive, and strategic manner. Identified weaknesses also pose challenges to the safeguarding of assets and data against loss and mishandling, and to full compliance with software license agreements.

Inventory Management and Tracking

The SAP Enterprise Asset Management (EAM) hardware module implemented in July 2017 has been appropriately tracking new hardware assets, but for legacy IT hardware assets purchased prior to this date, which represent 74% of HC and PHAC's hardware inventory, we found them to be insufficiently documented and tracked. As well, we found that 30% of laboratory IT hardware assets were not being tracked at all, as they did not always go through the IT warehouse receiving process. Overall, IMSD was unable to manage assets that they did not know existed, and the tools available were not sufficient to enable an electronic discovery of the IT landscape, thus requiring physical verification to account for all hardware assets.

Software asset information was being entered and tracked via a labour intensive and manual process in two separate systems, the SAP and SAM databases, neither of which offered a complete inventory of software assets, nor their licenses. Given that software assets reside on a variety of devices (computers, laptops, tablets), as well as on science-based devices not connected to the corporate network, this purely manual two-system process has proven to be inefficient, prone to errors, and unrealistic for the appropriate tracking of all software assets, and in particular, exposes HC and PHAC to legal and financial risks due to the potential mishandling of software licenses.

Relevant asset information was tracked in the APM Core system for business applications. We noted some incomplete and inaccurate data, but more significantly, we found that application support costs were not being tracked. Without support cost information, HC and PHAC's assessment of the technical health and business value of the asset was missing a key component to inform management action. Cost visibility enables HC and PHAC to optimize scarce resources and to ensure the business application portfolio is sufficiently healthy for the delivery of programs and services.

Monitoring and Maintenance

The complete inventory of low dollar value hardware assets (less than $10,000) has not been adequately monitored, as required by HC, PHAC, and Treasury Board Secretariat (TBS) Policy, Standards and Guides.

The capital IT assets included in the Annual Capital Asset Review (ACAR) were adequately monitored for departmental control, and their condition, which enables appropriate maintenance for departmental use, was adequately assessed. However, due to incomplete tracking of these assets in SAP, the ACAR exercise was not based on HC and PHAC's complete capital asset inventory.

We found that aging IT hardware assets were maintained through a 'break and fix' model, meaning they were repaired or replaced only when problems arose, thus leading to inefficiency and potential IT vulnerabilities.

We found that IMSD was monitoring and analyzing information about the state of existing business application assets and associated business and technical attributes, as well as engaging in activities to identify where the most attention was needed. Despite these efforts, there was no evidence that APM analytics and reports were being presented regularly to senior-level governance committees for consideration and direction, and there was little action or planning by application owners and technical advisors to adequately maintain business application assets for departmental use.

According to IMSD monitoring information, HC and PHAC has not met the TBS minimum target of 30% of the portfolio of business applications not requiring attention, and 80% of PHAC and HC's business applications were deemed to be aging. Given the substantial percentage of applications requiring some attention and the level of effort and resources required to address the aging situation, there is a risk that HC and PHAC may not be able to provide stakeholders with the well-maintained, secure, and available business applications that they require to deliver programs and services.

Disposal

Overall, we found that IT hardware asset disposals at HC and PHAC followed the established requirements, despite the fact that the published guidance was outdated.

The requirements and processes outlined by HC and PHAC for decommissioning business application assets were not being followed, nor was there a designated business process owner overseeing the process. Consequently, data residing in business applications was at risk of being mishandled or lost, and HC and PHAC are at risk of non-compliance with TBS requirements governing the disposition of data.

Background

1. HC and PHAC operate a shared services model where IT assets are managed by the Information Management Services Division (IMSD) within the Corporate Services Branch (CSB), which has custodial and managerial responsibility for IT assets. The other area responsible for IT assets is the Material and Asset Management Division (MAMD) within the Chief Financial Officer Branch (CFOB), which provides functional direction for applicable policies, as well as coordinating asset monitoring to ensure departmental assets are adequately managed.

2. The framework for IT Asset Management at HC and PHAC consists of a patchwork of supporting tools, processes, standards, controls and stakeholders that has been developed over time.

3. A follow-up audit was conducted in 2012-13 to the 2009 Audit of Information Technology (IT) Asset Management. The follow-up audit found that, while some improvements were noted in the development of the HC and PHAC Asset Management Policy suite, including monitoring of its compliance and the reconciliation, sanitization, and back-up process of surplus assets, further progress was required in the following areas:

   - completing an IT asset management framework and suite of procedures and directives;
   - reengineering all processes across the Agency to manage IT assets;
   - completing IT asset replacement strategies;
   - developing and implementing a comprehensive strategy to manage and control hardware and software inventories; and
   - implementing a tracking system for IT assets lent to staff.

4. These findings led to the implementation of significant actions, such as the annual monitoring of assets and the development of a suite of IT asset management protocols. The audit also highlighted the need to re-engineer ITAM processes and implement a strategy to manage and control hardware and software inventories.

5. Prior to 2017, IT assets were managed with the support of several legacy applications, including Lotus Notes for IT approval requests, HP Openview Asset Management (Asset Centre) for hardware assets, as well as the corporate financial system of record, SAP, to support the purchasing and financial reporting of the inventory of IT assets. Using these applications required repeated manual data entry in each of the systems, which resulted in inaccurate data being captured and applications that were difficult to reconcile with reporting and inventory tracking purposes.

6. With the aim of modernizing IT asset management and of consolidating IT asset information, an IT project was implemented July, 2017 to use the capability within SAP's Material Management and Plant Maintenance modules and to have the SAP Enterprise Asset Management (EAM) solution as the system of record for all IT assets at HC and PHAC. Implementing the hardware component required the migration of legacy data and the creation of new data entries. The software component of the project was later implemented in April 2018, but was found to be 'too cumbersome' as the process was manual, license tracking functionality was limited, and there was no discovery tool to enable the automated capture of

all software assets on the network. To address this gap, in 2018, IMSD developed and implemented a distinct tool (Access database) for software license management.

7. Following direction from TBS, IMSD also implemented the Application Portfolio Management (APM) Program and enabling tool (APM Core) in 2017, to ensure compliance with TBS reporting and analysis requirements for business application assets. According to IMSD, the APM Core tool was considered the repository for data on HC and PHAC's software assets and was intended as the single source of information for the tracking and monitoring of these assets. As the APM Program matures, it is becoming increasingly vital to ensuring the effective management of HC and PHAC's business application assets.

8. The appendices for this audit report provide additional information on the results of the audit and how it was conducted:
   - Appendix A – About the Audit;
   - Appendix B – Criteria; and
   - Appendix C – Scorecard.

Findings, Recommendations and Management Responses

Inventory Management and Asset Tracking

Inventory Management – Hardware

9. In September 2015, an investment project was launched to modernize the management of assets at HC and PHAC. The project was to use two modules in the existing corporate financial system (SAP) to manage corporate IT assets. These two modules, with additional added functionality, comprised the 'SAP Enterprise Asset Management' solution (SAP EAM).

10. Prior to implementation of this project, IT hardware assets were managed through the use of several legacy applications that required multiple entries resulting in inaccurate data and applications that were difficult to reconcile with reporting and inventory tracking purposes.

11. In July 2017, over 33,000 legacy IT hardware assets were migrated to the new SAP EAM hardware inventory database.

12. We expected to find an appropriate process in place for the receipt, inventory management, and distribution of IT hardware assets, and that the process was working as intended.

13. We found that there was an appropriate process in place for the receipt, inventory management, and distribution of IT hardware assets that were acquired after the implementation of the SAP IT hardware inventory within the EAM solution. IT hardware assets procured after July 2017, representing 26% of the IT hardware inventory, were found to be adequately received, tagged, and entered in the tracking system by the IT warehouse in the National Capital Region. The receipt and processing of IT hardware assets through the IT warehouse ensured that segregation of duties was maintained and that assets received met contract specifications prior to being deployed to clients.

14. The remaining 74% of the IT hardware inventory were assets that had been purchased prior to July 2017, or legacy assets that were migrated from Asset Centre into the new SAP IT hardware inventory. These IT hardware assets were found to be insufficiently documented and tracked, and could not be linked to procurement documentation. The inability to link these assets to their purchasing documentation, such as purchase orders, limited the ability to confirm that the goods received included in the new IT hardware inventory met client specifications and were accurately tracked prior to their deployment, thus affecting the overall reliability of the information in the IT hardware inventory.

15. We found that 30% of IT hardware assets in laboratories were not adequately received and tracked, as they were not tagged as HC assets, and were not accounted for in the tracking system. These assets were often received directly by the laboratories as part of 'laboratory equipment' related acquisitions and did not follow the standard receipt and deployment process through the IT warehouse.

16. By not adhering to an appropriate asset receipt, inventory management and distribution process, the Department's ability to accurately account for, and properly safeguard its complete inventory of IT assets was limited.

17. Finally, Standard Operating Procedures (SOPs) published on mySource for the receipt, inventory management, and distribution of IT hardware assets were not updated since the implementation of the new SAP EAM in 2017, and reflect outdated IT asset management procedures. While the processes outlined in the SOPs complied with Treasury Board requirements, the outdated SOPs still published for employee guidance could create confusion and lead to system entry errors, such as the incorrect creation of IT asset entries in SAP. Given that the SOPs did not reflect the new system entry workflow, following these outdated procedures would not enable accurate tracking of assets in the SAP IT inventories.

18. Legacy IT hardware assets acquired prior to July 2017, representing 74% of the IT hardware inventory, were found to be insufficiently documented and tracked, thus affecting the overall integrity of the IT hardware inventory. In addition, some IT assets in laboratories did not go through the IT warehouse receiving process. As a result, 30% of laboratory IT hardware assets surveyed were not tagged as HC assets, and were not accounted for in the tracking system.

Inventory Management – Software

19. In addition to IT hardware asset management, the newly implemented SAP EAM solution was also intended to modernize management of software assets. Unlike with hardware, there was no legacy system in place for the tracking of software assets prior to this project. As a result, software assets have only been tracked at HC and PHAC since April 2018.

20. As described in the project documentation, the newly implemented SAP EAM software component was to provide an "Inventory Management Solution where every software license is contained in one inventory and a full picture of what is in inventory and what is installed at a user's desk". Similar to the hardware inventory, the implemented software asset management process required manual system entry to create, update, and maintain the database.

21. However, the new solution was found to be too cumbersome to use, as its software license tracking functionalities were limited and did not meet software asset management requirements. These requirements included the ability to identify, detect, and report unused software assets, and the ability to discover and automate license detection. This ability to discover and manage licenses through an automated discovery function would have allowed for real-time identification of where licences were installed at any given moment. We found that this functionality was included in the SAP EAM project requirements, however it was not delivered.

22. This gap resulted in a separate Software Asset Management (SAM) database being implemented by IMSD in April, 2018 to manage the licences received and deployed. This database was also manual, and both systems (SAP EAM and SAM) were used to manage software assets (licenses).

23. **We expected to find an appropriate process in place for the receipt, inventory management, and distribution of IT software assets and that this process was working as intended.**

24. We found weaknesses in the tracking of software assets and licenses. As was the case with the IT hardware solution, we found that purchase order information could not be found for 51% of software assets tested (19 out of 37). As the software inventory only included assets purchased since its implementation in 2018, these findings indicate a lack of system controls for integration between the financial system and the new asset module.

25. We found that software orders were being entered in the SAP software inventory with a focus on completing the goods receipt process and closing the procurement loop for financial accounting and reporting purposes. Valuable software asset data, such as licence and assigned user information, was not being captured as intended in the SAP software inventory. For example, we found instances where licences were entered in 'batches' (e.g., multiple licenses entered in SAP under a single entry). In such cases, it was impossible to follow the receipt and deployment process of these licenses using SAP, leaving the system unable to accurately track software assets.

26. In cases where purchasing information was found, we attempted to reconcile these entries with IMSD's SAM license database in order to follow the complete receipt and deployment process. Overall, we found that 32% of the assets tested (12 out of 37) were adequately tracked using both the SAP software solution and SAM license database.

27. In summary, neither of the IT software tracking systems offered a complete inventory of software assets and licenses, either separately or together. The inability to appropriately manage software licenses exposes the Department and Agency to non-compliance with license agreements, to making misinformed purchasing decisions (e.g., under-using existing licenses), and to challenges in responding to vendor audits.

Inventory Management - Business Applications

28. In 2017, IMSD implemented the Application Portfolio Management (APM) Program and enabling tool (APM Core) to ensure compliance with TBS and to manage the business application assets. In developing and maturing the APM Program, the focus has been on collecting and analyzing the business application data, satisfying TBS reporting requirements, and organizing engagements with business application owners.

29. **For business applications, we expected to find that management and governance frameworks and applicable processes were in place and working as intended for inventory management.**

30. We found that many business application owners and technical advisors were not sufficiently engaged in managing the business applications, resulting in most business applications not having a maintenance plan. We also noted that there was varying levels of understanding

about the roles and responsibilities for updating the data within APM Core, and for planning and paying for the maintenance of business application assets.

31. We also found no Department and Agency policy or directive specifying the objectives of the APM Program, the authorities of stakeholders, the roles and responsibilities of key players, nor planning and reporting requirements.

32. Furthermore, we found no governance body focused on the APM Program, nor was APM a standing agenda item on any of the committees tasked with IT planning and resource allocation. In our review of governance committee minutes, we found little evidence of discussions or decisions related to the management of the existing portfolio of business application assets. The focus for governance appeared to be primarily on new applications. Without a governance framework to manage business applications, there is a risk that important business application initiatives may not be appropriately prioritized and fulfilled, that scarce resources may not be effectively allocated, and that cost-saving opportunities could be missed.

33. While there was a three-year IT plan for the period of 2019-22 prepared by IMSD for both HC and PHAC, there were no details identifying mitigation measures to manage business applications that were critical to operations, but that were not performing well and needed attention, nor how HC and PHAC were balancing investment decisions between existing portfolio needs and those of proposals for new applications. Without an integrated IT plan, with planned activities and costs identified for maintaining existing business applications, as well as for new IT initiatives, management does not have a complete view of HC and PHAC's IT portfolio and associated needs. This impedes the ability of senior management to make strategic decisions and to proactively manage and evaluate future investment as a portfolio.

34. In summary, there were elements in place of an appropriate process for the management of business application assets, but there were design weaknesses noted, along with a lack of governance support, which impeded the maturity of the APM Program and limited the process from working as intended.

Asset Tracking – Hardware

35. The Treasury Board *Policy on the Management of Materiel* requires that departments and agencies have a materiel management information system in place that enables the collection and generation of complete and accurate data that can support timely and informed materiel management decisions.

36. We expected to find an IT hardware asset management tracking system in place and that it contained accurate, reliable, and relevant information for decision making.

37. As noted in the previous section, we found that the newly implemented IT hardware inventory system was not reliable, as it did not contain a complete inventory of IT hardware assets nor did it provide accurate asset information to enable strategic IT decision making.

38. The tracking of IT hardware assets using a manual entry process has proven to be inefficient and has led to incomplete and unreliable IT hardware data. While we found the ‘HC network scan’ to be the most reliable discovery tool at HC and PHAC’s disposal, as it allowed for real-time discovery of 16,577 IT assets, the tool did not interface with the SAP EAM solution and required manual entry to update the asset information discovered. Although we found that all assets identified in the network scan were accurately tracked in the IT hardware inventory, the tool could only account for 27% of the computers listed in all of SAP, and 53% of the computers listed in the new IT hardware inventory.

39. We found that **14,808** of the computers in the new IT hardware inventory, and **20,473** of the computers in the rest of SAP were not identified in the network scan, and their existence and location could not be confirmed.

40. IMSD informed us that, while some of the IT hardware assets not identified in the network scan may have been new assets that were received but not yet deployed, they also may have represented assets that were permanently offline, or legacy assets that were no longer physically on HC and PHAC premises. They also noted that some of the these devices could also be assets still in use by the former First Nations and Inuit Health Branch employees, which was transitioned to Indigenous Services Canada, but have yet to be removed from the HC inventory.

41. We noted that the lack of completeness in the inventory was also attributed to various factors such as:
    - Legacy assets not being properly managed in the past and being difficult to track down;
    - The physical existence of IT assets was not confirmed prior to their migration from Asset Centre to the SAP hardware inventory. As a result, many assets in the inventory may be obsolete; and
    - Regions not following the new ITAM tracking process.

42. Furthermore, IMSD was unable to account for all IT hardware assets in the scientific digital environment, given that the network scan could not capture those assets that were not connected to the corporate network. A survey of HC laboratories conducted by the audit team identified 608 IT assets supporting HC laboratories being hosted on seven different science-based networks. Of these assets, only 177 (30%) assets were included in the new SAP hardware inventory.

43. The lack of sufficient system entry controls and database integrity allowed information to be entered in the wrong fields, for important asset information to be left uncompleted, and for human and system entry errors to go undetected. For example, out of the 59,760 assets in the new hardware inventory, only 49% of assets had an assigned user or location, with the rest of the assets being marked as missing or left blank. This level of incompleteness does not allow the data integrity needed to make fully informed decisions for the lifecycle management of IT asset. Another example was the discovery of duplicate asset tag numbers in the hardware inventory, as different assets were tracked with the same asset tag number. This increases the risk that the assets cannot be appropriately safeguarded, maintained, or monitored.

44. Due to a lack of accurate data, visibility of the IT landscape, and the lack of performance measures, the implemented SAP IT hardware solution does not effectively support informed IT asset decision making. Given that IT networks, infrastructure, and assets are highly movable and rapidly changing, updating the system using manual processes has proven to be a very difficult task, with unsatisfactory results.

45. The newly implemented SAP EAM hardware inventory module did not contain completely accurate, reliable, and relevant information for decision making. While all of the assets discovered on the network scan were accurately tracked in the SAP hardware database, the discovery tool could not account for all HC and PHAC computers and the new SAP hardware database did not account for all IT hardware, including legacy assets still in use and laboratory-based IT assets. Given that the new IT hardware inventory did not have an automated discovery functionality, updating the system was done manually, and proved to be a difficult and labour-intensive process. There was also no evidence that performance measures and targets for IT assets at HC and PHAC had been defined to measure the effectiveness of current and future asset management processes, for example, to review consumption and monitor age, costs, use, loss, and performance.

46. Overall, the current tools available to the Department and Agency are not sufficient to enable electronic discovery, resulting in an incomplete inventory of IT hardware assets.

Asset Tracking – Software

47. While we saw some recent improvements in the integrity of information captured in the SAP EAM solution for IT hardware assets (assets identified in the network scan and accurately tracked in the new hardware inventory), we did not see such improvements for software assets. This is largely due to the nature of the assets. IT hardware assets are physical assets and therefore more easily tracked by traditional asset management tools. Software assets, on the other hand, are intangible and require different tools.

48. As the implemented SAP inventory did not support automated discovery of software assets, the manual entry process implemented as part of the SAP EAM solution for the management of software did not meet software asset management (SAM) requirements. Because of the limitations in the SAP software inventory, and the lack of integrity in the data it holds, we were not able to conduct a comprehensive analysis of that inventory.

49. We expected to find a software asset management tracking system was in place and that contained accurate, reliable, and relevant information for decision making.

50. Our case studies conducted on IMSD's SAM license database demonstrated the challenges in manually managing thousands of software licenses that are in constant flux. Since neither the SAP software inventory nor the SAM database support automated discovery of software assets, HC and PHAC do not have adequate tools at their disposal to appropriately manage their inventory of software assets and licenses.

51. Given that software assets at HC and PHAC reside on a variety of devices (i.e., computers, laptops, tablets), as well as on science-based devices that are not connected to the corporate

network, a purely manual discovery process for software assets has proven to be inefficient, prone to errors, and unrealistic for the appropriate tracking of all software assets and licenses. For example, we found evidence of potential over-allocation of Markido Engage licenses when relying on the information captured in the SAM database (234 licenses were installed on computers, yet only 227 licenses were entered in SAM), and found that 16% of these licenses were assigned to the wrong user in the SAM license database. The use of unlicensed software or license over-allocation can lead to legal and financial risks for the Department and Agency, and highlights the importance of collecting accurate and timely software dates and information.

52. Furthermore, the information within the SAM license database was only able to account for 13% of all Visio licenses installed, and 20% of the listings in the SAM database were inaccurate (not installed on the computer assigned in the SAM database). While the SAM database has helped to mitigate some of the shortcomings of the SAP software inventory, it is incomplete and not able to fully account for HC and PHAC's complete inventory of software licenses in current use. Instances of multiple installations of the same perpetual Visio license on a device were also identified, demonstrating poor software optimization and ineffective use and allocation of software licenses.

53. Overall, the implemented SAP software inventory and SAM database did not enable HC and PHAC to appropriately and efficiently track software assets and licenses, nor did they contain complete and accurate information for decision making. These gaps expose the Department and Agency to legal and financial risks.

Asset Tracking - Business Applications

54. Corporate oversight and informed decision making require accurate and complete data. The APM Core tool is the repository for data on HC and PHAC's business application assets, and is intended to be the single source of information for the tracking of these assets.

55. We expected to find that a business application management tracking system was in place and contained accurate, reliable, and relevant information for decision making.

56. We found that, while there was a tracking system in place (APM Core) for business applications, we noted a range of data completeness and quality issues, mostly evident in the data fields for stakeholder information, application status, and planned decommissioning date. While significant effort has been made to track and analyze business application information to enable decision making, the reason that the data was not sufficiently accurate and reliable was because of a lack of rigour and consistency being applied across branches in collecting and updating asset information. IMSD Client Engagement teams were each assigned a group of business application owners, but the nature, extent, and timing of engagement varied by team, resulting in data not always being up-to-date, data entry errors, and uneven collection of data. In addition, we found a lack of manual and automated internal controls in place to prevent and detect data errors in APM Core.

57. We also found that application support costing, which is a relevant component for meaningful assessment and management of the business application portfolio, was not being tracked in

APM Core. While there is a field in APM Core for cost data, there was no policy or governance requirement to track or support cost data, no requests from IMSD for business owners to provide such data, nor any costing formula and supporting guidance from which to derive an accurate calculation of support costs. We further noted that at HC and PHAC, it was the practice for new business applications to be released into production without consideration and budgeting for ongoing maintenance and support costs. Without support costs being tracked, the TIME Assessment (Tolerate, Innovate, Mitigate, and Eliminate) that was meant to track the technical health and business value of the asset for decision making was missing a key component to inform management action. Cost visibility enables HC and PHAC to optimize their scarce resources to ensure that the business application portfolio is sufficiently healthy for the delivery of their programs and services.

58. Business application assets were being tracked by the Application Portfolio Management (APM) Program and its enabling system, APM Core. However, the business application information being tracked was not sufficiently accurate, reliable, or relevant for decision making due to process control gaps, inconsistent engagement by business owners, and lack of insight into application support costs.

Recommendations for Inventory Management and Asset Tracking

Recommendation #1. The Assistant Deputy Minister, Corporate Services Branch (ADM-CSB), and the Health Canada Chief Financial Officer (CFO) should ensure that all Information Technology (IT) assets are appropriately tagged for inventory purposes, that a baseline inventory count of IT assets is conducted, and that the Systems Applications and Products (SAP) IT inventory data is updated accordingly, including the removal and transfer of the Indigenous Service Canada assets from HC's inventory. These actions will ensure that HC and PHAC's complete inventory of IT assets can be accurately accounted for and properly safeguarded.

Recommendation #2. The ADM-CSB and HC CFO should update Department and Agency Information Technology Asset Management (ITAM) policies, guidance, and standard operating procedures, including a definition of IT assets and lab equipment, to reflect current practices and systems, and to comply with Treasury Board policies for IT hardware, software, and business applications. At a minimum, the objectives of ITAM, the authorities of stakeholders, and the roles and responsibilities of key players should be specified, to ensure sufficient engagement of stakeholders in effectively managing IT assets.

Recommendation #3. The ADM-CSB should integrate ITAM governance and planning into HC and PHAC's current governance framework and their enterprise planning cycle and framework to ensure that IT assets get the attention, resources, and decisive action required to be managed effectively.

Recommendation #4. The ADM-CSB and the HC CFO should re-assess the current software asset tracking processes and systems and establish an integrated solution. The integrated solution should support effective management of software assets throughout their lifecycle, eliminate the need for duplicate entry of software asset data into the various tracking systems, provide an automated discovery functionality, and enable linkages to other supporting information, such as purchasing documentation, software licenses, and maintenance costs.

Recommendation #5. The HC CFO and ADM-CSB should ensure that sufficient business process and application controls are implemented within the asset tracking and monitoring systems for IT hardware, software, and business applications in order to reduce data entry errors and ensure the completeness, reliability, and relevance of IT asset data. (EAM SAP, SAM, and APM)

Recommendation #6. The HC CFO, PHAC CFO, and ADM-CSB should ensure that a funding formula for support and maintenance costs of existing business applications is established, that future ongoing maintenance costs are included in the full cost of new business applications, and that required funds are budgeted accordingly. These actions will support well-informed decision making for the ongoing health of the business application portfolio.

Management response

Recommendation #1
Management agrees with the recommendation.

Since 2017, all IT assets that have financial (beyond a nominal low dollar threshold) or business value (all procured assets that could contain data, including computing and storage devices) are being tagged and tracked.

A new enterprise asset management system is under development with the intent to be made operational in Q3 2022-23. This will put in place additional measures to track the operational use and safeguarding of assets. SAP will remain the authoritative information source for retaining and managing financial information associated with assets.

While an enterprise asset management system is under development, additional measures will be put into place to track the operational use and safeguarding of assets. Coordination and liaison will include continued engagement with business owners, including those in laboratory environments, to ensure proper handling of all assets.

In addition, technologies are in place that mitigate the risk of information being mishandled. Such technologies include the continued use of CSE capabilities, including host and network-based sensors, as well as internal capabilities, including bitlocker and positive control of USBs.

Recommendation #2
Management agrees with the recommendation.

The Health Canada Standard on Asset Management defines IT assets as: “Equipment that is supported by the Information Management and Services Directorate, including computers, monitors, laptops, printers, scanners, external hard drives, projectors, BlackBerry/PDA devices, servers, and server equipment." It also states that specified labs are responsible for activities related to the acquisition, barcoding, and disposal of laboratory assets. Assets within labs that have digital components do not fit the definition of IT assets and would not be subject to IT asset management. CSB and CFOB will work with DGs responsible for laboratory operations to ensure all assets are accounted for and that the necessary safeguards for information are in place.

Recommendation #3

Management agrees with the recommendation.

There are a number of governance discussions that form part of the overall investment planning and IT planning cycle. The enterprise architecture team presents Application Portfolio Management (APM) data to individual branches to inform branch operational planning in order to feed the departmental investment planning process. This culminates in Executive Committee-level investment decisions for capital assets and projects. The annual IT planning process complements the investment planning process and identifies risks and investment opportunities aligned to support the digital modernization framework. These are both reviewed through departmental governance bodies and approved by the Deputy Head.

A key aspect of HC departmental IP governance is the role of the DG-level subject-matter expert leads for the four asset classes. One of the four asset classes is the area of IM/IT which oversees IT assets and is led by Health Canada's CIO. Investments in IM/IT that are material in dollar value and/or higher in risk are brought to IP governance for approval and assigned appropriate capacity and resources.

Starting in July 2021, PHAC has created a VP level committee for Resources and Operations which is responsible for monitoring and oversight of investment planning. This includes Governance and oversight of financial resource allocations, investment decisions, and G&Cs, as well as provision of a challenge function for branch and Agency financial, operational, and resource planning (procurement, IT, accommodations, etc.), and monitoring of ongoing implementation of approved plans to ensure alignment between operations, spending, and results for the overall achievement of Agency priorities and results.

Recommendation #4

Management agrees with the recommendation.

CSB provides software management for both Health Canada and PHAC with procurement currently managed in SAP with input derived directly from the Service Gateway: https://servicegateway-passerelledeservice.hc-sc.gc.ca/en/software.html.

SAP does not offer the same functionality as other software asset management tools, and management agrees that a new system is needed to more effectively manage software. It is reassuring, however, that a 2019 KPMG audit on behalf of IBM found compliance in 120 of 125 instances. This provides a reliable indicator that the governance, policies, and processes in place for software asset management for Health Canada and PHAC are in a relatively good state.

CSB will work with CFOB on improving software lifecycle management. A review of existing tools and processes as part of a gap analysis will be considered in the identification of requirements for an integrated SAM solution to digitize the business process to support data integrity in the support of asset management.

Recommendation #5

Management agrees with the recommendation.

A distinction needs to be made between management of business applications, IT hardware and software. Hardware and software will be addressed through the adoption of a new ITAM system.

Enhanced ITAM (software and hardware) capabilities, processes, and data management and integration will be delivered under a new ITAM capability where human errors will be minimised through the use of automation capabilities provided by the tool. Data quality will also be improved by the deployment of a Discovery capability which will find and identify IT hardware and software assets on the network, providing real-time asset identification and tracking.

In addition to CSB implementing an independent ITAM solution for tracking and monitoring hardware and software, CFOB will review current (SAP) system entry controls to determine if any further user typing entry errors can be flagged, and initiate a SAP system change request accordingly

As the audit notes, the process for managing and tracking the data for our business applications is good but not consistent, leading to some data quality issues. There is also room for greater engagement with stakeholders, including governance bodies, in the APM tracking and management of business applications. Since its introduction in 2017, however, the APM program has evolved in the management of business applications with HC and PHAC having received favourable MAF scores for our overall level of IT maturity which includes APM as an assessment factor.

Recommendation #6

Management agrees with the recommendation.

Increasingly, measures are in place to ensure ongoing maintenance costs are factored into decisions about business applications. Departmental governance ensures on-going costs as per agreed model in Transition Plans for new business applications. This is a prerequisite for Gate 4 sign off as per the Department Project Management Framework (DPMF). In response to the recommendation that future ongoing maintenance costs are included in the full cost of new business applications, in collaboration with IMSD, CFOB created a departmental IT Project costing tool in 2020 to determine the cost of new business applications, which was approved by departmental governance. This tool includes a component to calculate future ongoing maintenance costs. Once the ongoing maintenance costs are calculated, funding decisions are made. If the business application is part of a request for funding from the fiscal framework, the funding for ongoing maintenance costs is included in the Budget ask and related TB submission.

The IT Project costing tool can also be used to determine ongoing costs for existing business applications. For existing business applications, the source of funds for ongoing maintenance costs has been established. In the circumstance where the source of funds is insufficient, the IT Project costing tool can be used to determine the resource need, and funding requests can be brought to departmental governance to seek additional funding. The Department will continue to examine aging IT business applications as part of the annual reporting to TBS and assess risks associated with ongoing maintenance costs.

The IT Systems Development Management Framework applies to new and changed business applications and includes the completion of a Transition Plan (noted above). The Framework was accepted as a completed deliverable as part of Audit of IT Systems Development MRAP. The Quality Assurance process to enforce compliance is currently being finalized to close off that MRAP.

Monitoring and Maintenance

Monitoring – Low Dollar Value and Capital IT Assets

59. The Treasury Board *Policy on Management of Materiel* and the applicable TBS guidance document state that departments and agencies should conduct regular physical verifications of assets. HC and PHAC's Standard on Asset Management and the Asset Inventories Instruction Guide state that the Department and Agency must conduct regular physical verifications of their assets. HC and PHAC conduct two separate departmental assets inventory verification exercises annually. An Assets Inventory Verification Exercise (AIVE) of assets valued at less than $10,000 is conducted every three years, with the last one having taken place in 2017, and an Annual Capital Assets Review (ACAR) of assets valued $10,000 and greater. As per the HC and PHAC Asset Inventories Guide, all IT equipment such as computers, monitors, fax machines, printers, scanners, etc. should be verified as part of the AIVE. All software items were excluded from this exercise. All capital IT assets, hardware, and software valued $10,000 and greater were accounted for as part of the Annual Capital Asset Review.

60. These inventory exercises relied on the asset information recorded in the SAP EAM tracking system to conduct 100% monitoring of assets. Within SAP, there were two types of asset records: Equipment Master Records (EMRs), created for all assets valued at $1,000 and above (including all capital assets and attractive assets), and an Asset Master Record (AMR), created for capital assets only (those valued at $10,000 and above).

61. To launch the monitoring processes, MAMD generates capital asset lists (based on AMR records) and low dollar value asset lists (based on EMR records) per cost centre, and sends the inventory lists to cost centre managers for their validation and verification.

62. We expected to find that IT assets were adequately monitored and that monitoring results are actioned.

<u>Low Dollar Value (LDV) IT Assets (AIVE)</u>

63. While HC and PHAC monitoring processes were well documented and in alignment with the Treasury Board Policy on Management of Materiel, our testing of these processes demonstrated that monitoring of low dollar value IT assets at HC and PHAC had not been

taking place. Although MAMD had conducted an AIVE exercise, all IT assets, both hardware and software, were excluded from the list of assets reviewed, which is in contravention of the above noted policies and guidance. No other monitoring exercise for low dollar value IT assets has taken place.

64. As the AIVE excluded IT assets from its verification exercise, we found that there was no process in place to ensure that HC and PHAC's inventory of low dollar value IT assets, such as USB sticks, servers, laptops, tablets, computers, and monitors were well managed, properly accounted for, and recorded in SAP, as per HC and PHAC policy. This lack of monitoring increases the risk that LDV IT assets are not properly safeguarded and exposes the Department and Agency to risks of asset misuse, lack of maintenance, and theft. These risks are heightened by the fact that hardware assets may contain sensitive information, which if not accounted for, could result in privacy, IM/IT, and cybersecurity risks.

Capital IT Assets

65. While IT assets were not included as part of the AIVE, we found that capital IT assets were included in the Annual Capital Asset Review (ACAR), as required by HC and PHAC's Asset Management Standard, the Asset Inventories Instruction Guide, and the TB Policy and Guide to Management of Materiel. As part of the 2018-19 ACAR, assets with a combined acquisition value of $55,744,051 were appropriately monitored. However, the design of the ACAR process relies on the integrity and completeness of data captured for capital assets in SAP. Given the challenges of ensuring that accurate and reliable information was captured within the SAP EAM system, we found that capital IT assets that were miscoded or not accurately captured in SAP did not appear on the inventory lists used to conduct the ACAR, and were not accounted for as part of the monitoring process.

66. We found 384 IT assets, with acquisition values of $10,000 or above, that had not been included in the 2018-19 ACAR. Reasons provided for these discrepancies include improper coding, human error in data entry, and lack of system entry controls that resulted in duplicate or obsolete asset entries (i.e., assets that had not been adequately disposed or deactivated).

67. In addition, while the Standard on Asset Management clearly outlined that MAMD should 'physically verify assets themselves' during the ACAR, guidance on the selection of assets to be verified was broadly stated and did not help ensure that the sample selected was representative of the complete capital IT asset population. As a result, we found that only one software capital asset was physically verified by MAMD during the 2018-19 ACAR, thus not providing sufficient oversight of the process.

68. We also noted that unclear roles and responsibilities between IMSD and MAMD have caused confusion and noncompliance with monitoring requirements. This created further confusion as capital IT assets were monitored by MAMD, but low dollar value IT assets were excluded from their review, as it was stated that IMSD held 'custodial and managerial' responsibility for all IT assets.

69. Overall, enhanced system entry controls are needed to ensure that the Department and Agency can account for and monitor their complete population of IT assets.

70. The complete inventory of low dollar value IT assets has not been adequately monitored, as required by HC and PHAC Asset Management Standard, the Asset Inventories Instruction Guide and the TBS Policy and Guide to Management of Materiel. IT assets were not included in the Assets Inventory Verification Exercises and no other monitoring exercise took place to ensure that low dollar value IT assets were adequately managed.

71. Capital IT assets included in the Annual Capital Asset Review (ACAR) were adequately monitored and accounted for as part of the exercise, and their ‘condition’, which enables appropriate maintenance for departmental use, was adequately assessed. However, due to an incomplete IT population in the SAP asset management database, the ACAR could not account for all Capital IT assets. As such, the ACAR exercise did not account for nor assess the condition of the complete capital IT asset inventory. We also found that insufficient physical verifications were conducted by MAMD as only one software asset was physically verified during the last review.

Monitoring and Maintenance - Business Applications

72. In order to monitor the health of HC and PHAC’s portfolio of business application assets and to transmit APM data to TBS annually, the APM Program was designed to monitor and assess the technical condition and continued business value of each business application being tracked by conducting an aging IT assessment and designating each business application into one of four action categories of the TIME assessment: Tolerate, Innovate, Mitigate, or Eliminate. To ensure adequate maintenance of business applications and to manage aging IT, TBS established a minimum target for departments that 30% of the business application portfolios should not require attention. HC and PHAC report on this target annually to TBS.

73. We expected to find that business application assets were adequately monitored and maintained. Specifically, we expected IMSD to have engaged with business owners in monitoring the health of business applications and to provide information, analytics, and advice to business owners, as well as governance, in a timely manner for their consideration and action. We further expected business application owners to have an action plan to maintain their portfolio of assets, to meet or exceed the TBS minimum target, and to address their aging IT.

74. We found that IMSD had engaged with business application owners and technical experts throughout the year via several monitoring activities to gather the necessary updates to business application information in APM Core, to conduct assessments, to help business owners understand the status of their business applications, and to identify where attention was needed. These efforts enabled IMSD to perform TIME and aging analyses of the business application portfolio, to provide timely transmission of APM data to TBS, and to produce an annual Branch Application Portfolio Analysis Report. However, there was no evidence that APM analytics and reports were being presented regularly to governance for their consideration nor that any requisite direction was provided to business owners.

75. We found that business applications were being monitored by IMSD, but that the degree of rigour and consistency applied during these activities varied across branches, IMSD client

engagement teams, and technical advisors, thus potentially reducing the accuracy and confidence in the results. Also, despite IMSD's efforts, we found that appropriate actions and planning to adequately maintain business application assets for departmental use were not always being taken, and most business owners and branches did not have a strategy or action plan for maintaining their business applications. According to IMSD monitoring information, HC and PHAC have not met the TBS' minimum target of 30% of the portfolio of business applications not requiring attention (maintenance, upgrade, replacement, decommission, etc.), with PHAC and HC respectively at 15% and 27.2% as of September 2019. Also, according to IMSD's aging IT assessments, 80% of PHAC and HC's business applications were aging (generally referring to applications that are based on outdated software that relies on technical expertise that is increasingly scarce and supported by old infrastructure that is becoming increasingly more expensive to operate).

76. We found that there was no departmental or agency authority actively overseeing and holding business owners to account for the maintenance of the business application portfolio of assets. We also found that the focus at all levels across the Department and Agency has been primarily on delivering new business applications, and satisfying TBS' annual reporting requirements on the health of the business application portfolio. There was a lower priority assigned to maintaining the existing applications that were sustaining programs and service delivery. The attention and resources required to manage existing business applications were competing against these new applications, along with mandatory GC initiatives, for the same resource pool.

77. Despite IMSD's efforts to monitor, analyze, and prepare business application asset information, and to engage and advise business application owners, these assets were not being adequately maintained. Given the substantial percentage of applications requiring some attention and the level of effort and resources required to address the aging situation, there is a risk that HC and PHAC may not be able to provide stakeholders with the well-maintained, secure, and available business applications required to deliver programs and services.

Monitoring and Maintenance - Aging Hardware

78. According to the TB Policy on the Management of Materiel, preventive maintenance should be designed to preserve and enhance equipment reliability by replacing worn components before they fail. This is usually achieved by the implementation of an evergreen IT process that continuously replaces or upgrades IT hardware according to a planned refresh schedule in order to ensure that equipment remains relevant, secure, and up-to-date.

79. We expected to find IT assets were adequately maintained.

80. IMSD stated that it did not have the resources to carry out an effective evergreening program at HC and PHAC. Instead, aging hardware was primarily maintained through a "break and fix" approach. In November 2018, IMSD estimated that 55% of deployed primary computing devices at HC and PHAC were past warranty and at risk of failure, as compared to the industry standard average of 20%.

81. Through analysis of the Asset Management Database in SAP, we found evidence of many 'legacy' aging hardware assets that had not been identified for disposal in a timely manner. IMSD explained that while many of these assets may be obsolete, the lack of an evergreening program, in addition to many years of inadequate record keeping, have affected the integrity of asset information in SAP, and has limited the Department's ability to proactively identify IT assets for disposal. For example, a replacement date analysis of the newly implemented IT hardware inventory revealed that only 27% of computers and tablets listed in the inventory have a 'replacement date' indicated in their asset entry, with over 22,900 computers and tablets in the inventory not having such a date recorded.

82. The ability to effectively address IT issues was also hindered by limited information on IT and aging IT performance measures, as well as undefined performance targets. While limited asset performance information was collected for capital assets included in the Annual Capital Asset Review (ACAR), there was no such similar process in place for low dollar value IT assets, as the AIVE was not being conducted for IT assets. We found no process in place to adequately assess the condition of all hardware IT assets and collect performance information that could enable their timely maintenance, help ensure that assets are used as effectively and efficiently as possible to optimize the value provided by their use, and identify them for disposal as soon as they become surplus to the requirements of program delivery.

83. As disposal decisions were not being informed by an inventory cost-benefit analysis, we found that legacy hardware assets were not identified for surplus or disposed of in a timely manner. For example, we found 19,541 computers and tablets that had a "replace by" date of 2018 that had not yet been disposed. In this example, the computer equipment not identified for disposal in a timely manner may have gone beyond its useful lifecycle and not be of any use for the Computers for Schools program.

84. Aging IT hardware also poses IT security risks, as it is vulnerable to the loss of technical support on these legacy systems, increasing the risk of successful cyberattacks. For example, Microsoft ended support for its Windows 7 operating system on January 14, 2020, meaning the company will no longer provide any new security updates and support. This created potential security risks for HC and PHAC systems, as well as for applications still being run on Windows 7, as they become more prone to malware and hacking. New operating systems, such as Windows 10, also present a challenge for the Department and Agency, as aging hardware becomes incompatible with the new technology (i.e., some computer hard drives could not support running the Windows 10 operating system and needed replacement). These challenges and risks could have been reduced with the adoption of an evergreening program.

85. We found insufficient controls in place for the maintenance of IT hardware, given that the process was reactive in nature. Aging IT hardware assets were maintained through a "break and fix" model, and were only repaired or replaced once problems arose, thus leading to inefficiency and potential IT vulnerabilities. Given today's increasingly sophisticated cyber threats, it is important for HC and PHAC to not only account for all assets in their digital environment, but also proactively repair, support, or replace damaged assets in a timely manner.

Recommendations for Monitoring and Maintenance

Recommendation #7. The CFO, in collaboration with the ADM-CSB, should ensure that monitoring activities for low dollar value IT assets follow the updated guidance in order to safeguard private and public information contained therein.

Recommendation #8. The ADM-CSB should ensure that the following steps are taken in order to meet TBS targets, and to address the 80% of business applications deemed to be aging, in an efficient and fully informed manner:

- Ensure branch business application owners take immediate action on business applications deemed as ‘needing attention’ and or ‘critical’, and develop detailed maintenance plans for remaining business applications for their integration into the IT plan, and into the enterprise planning and budgeting cycle;
- Incorporate aging IT as a regular governance agenda item;
- Clarify roles and responsibilities for aging IT systems;
- Establish performance measures to oversee and report on progress; and
- Establish a project with requirements and direction for modernizing the portfolio of business applications.

Recommendation #9. The ADM-CSB, in collaboration with senior management, should develop a strategy to address aging IT hardware issues proactively, which may include the establishment of an IT hardware evergreening program, and should include the establishment of performance measures and targets to monitor and report on HC and PHAC’s progress in addressing aging IT risks, in making informed IT disposal decision, and in ensuring the continued achievement of operational objectives and program delivery.

Management response

Recommendation #7
Management agrees with the recommendation.

The audit highlights a lack of control of assets and the subsequent risk of a possible loss of control of private and public information. It was noted by management, upon review, that the information residing on these low dollar assets is secure based on the below evidence.

Information on USB keys is secure:

- Loss of control of USB keys and information stored on USB keys was specified as a potential risk. Since 2014, only secure USB keys have been able to connect to departmental devices. Information on a secure USB key would not be accessible if the device were lost or stolen as it could not be accessed without the PKI credentials of the owner. It is also not possible to use a non-issued USB key on government computing devices.
- All other USB mass storage devices are prohibited, unless approved for whitelisting by IT Security. A BNews was sent on April 22, 2014.

All Health Canada and PHAC devices are encrypted to protect information if a device is lost, stolen or other inappropriate access:

- Bitlocker encryption was introduced to HC/PHAC computers as part of the Windows 7 upgrade in 2014-15 and continues to be in place. Bitlocker protects data on computing devices by preventing unauthorized access to the hard disk drive and the information therein.

All Health Canada and PHAC computers have CSE sensors installed to allow monitoring of devices against theft, unintentional or intentional access attempts:

- CSE implemented Host Based Sensor (HBS) capabilities in Q1, 2015. These sensors exist on computing devices and detect any unintended / malicious / unapproved attempted accesses if connected to any network. HBS capabilities were further enhanced with the implementation of Network and Cloud-based sensors in subsequent years to protect other back-end elements of HC/PHAC IT Infrastructure.

CFOB will review the current ITAM policy on attractive and trackable low dollar assets. Accountabilities for ADMs and other stakeholders will be clearly articulated in any revised policies and directives.

Recommendation #8

Management agrees with the recommendation.

Governance related to application management is more mature than represented. The audit report highlights the Application Portfolio Management (APM) of IMSD as having a lack of engagement with clients at governance bodies. It must be noted that there are a number of discrete governance discussions that form part of the overall investment planning and IT planning cycle.

The APM team presents APM data to individual branches to inform branch operational planning in order to feed the departmental investment planning process. This culminates in Executive Committee-level investment decisions for capital assets, IPs and targeted vulnerabilities or DM reserve requests.

The annual IT planning process complements the investment planning process and identifies risks and investment opportunities aligned to support the digital modernization framework. These are both reviewed through departmental governance bodies and approved by the Deputy Head.

There is a defined process to support application management work plans:

- A process is already in place as part of annual TBS reporting to address aging IT and is included in the decision-making process for investment planning, working with existing governance tables. Aging IT and TIME assessment reports are delivered to management teams which are then used to drive annual planning. There is no requirement to stand up a new project with requirements and direction for modernizing the portfolio of business applications as this framework currently exists.

- The Workload Migration and Modernization (WLM) Project plan was to migrate business applications from Legacy environments to the end state by March 2023. Early environmental review for HC and PHAC was prepared by Accenture. As of November 2021, this is now being lead by TBS and SSC with a working group of CFOs and CIOs to assess the overall risk and path forward for the GC Cloud Strategy and Financial Model.

- Business applications have a well-established processes in use by IMSD and program business owners, with results reported to TBS. HC and PHAC have received favourable MAF scores for our overall level of IT maturity which includes APM as an assessment factor.

Recommendation #9
Management agrees with the recommendation.

In fiscal year 2020-21 CSB implemented an IT hardware evergreening program for computers based on a five-year amortization cycle for HC and PHAC.

CSB will continue to engage stakeholders and evolve the evergreening strategy as this develops with SSC as part of Enterprise IT.

Asset Disposal

Asset Disposal - Hardware

86. Appropriate asset management ensures that assets found to be unrepairable, no longer performing as intended, or being replaced to support the implementation of sustainable projects, such as IT evergreening, should be identified for surplus in a timely manner. The overriding disposal objective is "to ensure the disposal of surplus materiel assets is concluded as effectively as possible, as soon as possible after they become surplus to the requirements of program delivery, in a manner that obtains highest net value for the Crown, and in compliance with the Treasury Board Directive on Disposal of Surplus Materiel." From an IT security perspective, there are also important benefits to disposing of vulnerable assets that are no longer being supported in a timely and effective manner.

87. We expected to find the internal disposal process was aligned with the TB Policy on Management of Materiel, and ensured that the disposal of surplus IT assets was concluded as effectively and in as timely as fashion as possible. We also expected to find that HC and PHAC supported the ‘Computers for Schools’ (CFS) program and disposed of all computers in compliance with the CFS guidance.

88. Our assessment of the disposal process in place for hardware assets at the IT warehouse demonstrated that the controls in place effectively supported the achievement of appropriate hardware disposal. The process was assessed, met TB policy requirements, and complied with the ‘Computers for Schools’ program, as all computer equipment tested was adequately processed, documented, and sent for surplus using appropriate mechanisms, thus enabling efficient re-use of resources.

89. We were also able to determine that adequate controls were in place for the hard drive sanitization practices that took place prior to disposal, as asset hard drives were appropriately wiped and certified for surplus prior to disposal. Such controls helped ensure the protection of departmental information.

90. However, we found that published employee guidance and standard operating procedures were outdated, reflecting the previous disposal process in SAP. Adherence to these outdated procedures could lead to system entry errors, further affecting the integrity of the information in the SAP hardware inventory.

91. We found that, overall, IT hardware asset disposals at HC and PHAC followed the established requirements; however, published guidance was outdated.

Asset Disposal - Business Applications

92. HC and PHAC have a decommissioning process for business applications, along with a step-by-step approval form that incorporates the TBS requirements governing the disposition of data residing in business applications and databases. The business application owner, with assistance from IMSD, determines and recommends the decommission plan that best suits the data retention and operational requirements. The plan is reviewed by an Information Management (IM) Specialist, and approved by the business application owner and the respective Director General.

93. We expected IT asset disposals to follow HC and PHAC requirements. For business applications, we further expected that action was taken and plans made to decommission those business applications that were deemed as “Decommissioning Pending”.

94. We found that the requirements and process outlined by HC and PHAC for decommissioning business application assets were not being followed. Despite a detailed process and tool (a decommissioning form) to assist the business owner, the lack of a designated owner to oversee the decommissioning meant that there was no enforcement of the process. There was no formal, standardized communication with business owners following the designation of a business application as decommission-pending, nor was there evidence of any follow-up to determine whether the business application was indeed decommissioned, and if so, if was it done according to requirements.

95. Our testing of business applications identified as ‘decommissioning pending’ in APM Core revealed that most had not been actioned for decommissioning, or if they had, the process for decommissioning had not been followed appropriately, nor was there evidence of a decommissioning form in the process of being completed and approved or of a decommissioning plan. Data stored in these business applications was at risk of being mishandled and of being unavailable for Access to Information and Privacy (ATIP) requests, legal and investigative proceedings, and future business value. Prior to removing a business application from the network, it is important to ascertain whether the data must remain accessible and handle it accordingly.

96. Our testing also indicated that the ‘decommission’ status information in APM Core was not reliable. Of the 258 business applications being tracked in APM Core, 19 were identified as ‘decommission pending’. However, of those 19, only eight had a decommission date, two of which were past due. As well, according to APM Core, there were 15 applications designated as ‘in production’, but also with a decommission date that was past due.

97. The requirements and process outlined by HC and PHAC for decommissioning business application assets were not being followed, nor was there a designated owner overseeing the process. Consequently, data residing in business applications was at risk of being mishandled or lost, and HC and PHAC were at risk of non-compliance with TBS requirements governing the disposition of data.

Recommendation for Asset Disposal

Recommendation #10. The ADM-CSB should identify a business process owner with appropriate authority to oversee and enforce compliance of the decommissioning process for business applications. This action will reduce the risk of important data residing in business applications from being mishandled or lost.

Management response

Recommendation #10

Management agrees with the recommendation.

Enterprise Architecture (EA) within CSB is the business process owner for application decommissioning.

EA already has an application decommissioning strategy that was developed in consultation with groups within and outside of IMSD, followed by Business Owner engagement through various pilots in 2019-20. More formal implementation of that strategy began in 2020-21, with a written description of the decommissioning process and associated client form being available on GCPedia.
Direct stakeholder engagement to communicate the decommissioning process and underlying expectations is still needed, including socialization and integration into IT investment projects through the various governance tables.

Conclusion

98. Overall, while we noted some positive aspects of the management of hardware assets and business applications, we found incomplete and inaccurate asset data in each of the IT asset supporting systems, along with inadequate governance support, planning and engagement for IT asset management. These gaps impeded HC and PHAC’s ability to make fully informed decisions about asset investment, maintenance, disposal, and how to focus on prioritizing and fulfilling asset initiatives in a cost effective, proactive, and strategic manner. As well,

identified weaknesses pose challenges to the safeguarding of assets and data against loss and mishandling, and to complying fully with software license agreements.

Appendix A – About the Audit

Audit Objective

The objective of the audit was to provide reasonable assurance that appropriate controls are in place for IT asset management.

Audit Scope

The audit included the examination and assessment of all relevant systems, records, personnel, and physical properties related to HC and PHAC IT assets up to June 2019.

Activities not in Scope

The scope did not include:

- Detailed testing of IT asset planning and acquisition phases, as an audit of contracting and procurement was performed during fiscal year 2018-19 and an audit of investment planning was scheduled for fiscal year 2020-21;
- Telecommunication equipment, such as Blackberries and cellular phones, will not be included, given that they are under the purview of Shared Services Canada;
- IT assets within the National Microbiology Laboratory (NML), as the NML and HC have an established Memorandum of Understanding regarding the management of IT assets. The NML's laboratory IT assets are managed independently of IMSD. As such, there are risks related to the independent nature of the management of the IT assets, as well as risks related to the Level 3 and 4 labs related to possible contamination of IT hardware assets and the processes in place to dispose of them. In order to keep the scope manageable and complete this IT asset management audit within a reasonable time, the NML was scoped out and will be reassessed for a future audit during the Risk-Based Audit Plan (RBAP) process.

Audit Approach

The audit was conducted in accordance with the Government of Canada's *Policy on Internal Audit*, which requires examining sufficient and relevant evidence, and obtaining sufficient information and explanations to provide a reasonable level of assurance in support of the audit conclusion.

The audit criteria were derived from the Comptroller General's Audit Criteria related to the Management Accountability Framework: A Tool for Internal Auditors (2011), the Health Canada and Public Health Agency of Canada Standard on Asset Management, and the TB Guide to Material Management.

The audit approach included, but was not limited to:

- Interviews with Information Management Services Division (IMSD), Material and Asset Management Division (MAMD), branch laboratories within the National Capital Region, and regional laboratory officials responsible for the receipt, maintenance, monitoring, and disposal of IT assets;

- Review of relevant documentation, policies, standards, guidelines, and frameworks related to the asset management lifecycle;
- Walkthroughs and control design testing of select key controls;
- Detailed testing of a sample of IT assets; and
- Analysis of findings from interviews, inquiries, document reviews, and detailed testing.

The project was collaborative and the findings were cleared with the parties concerned.

Statement of Conformance

This audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing, as supported by the results of the Office of Audit and Evaluation's Quality Assurance and Improvement Program.

Appendix B – Lines of enquiry and criteria

Audit of Information Technology (IT) Asset Management

Criteria Title	Audit Criteria
Line of Enquiry 1 – Inventory Management and Tracking Criterion #1: IT assets were appropriately received and tracked to ensure information was accurate, reliable, and relevant for decision making.	
Sub-criterion – #1.1	It was expected that an appropriate process was in place for the receipt, inventory management, and distribution of IT assets, and was working as intended.
Sub-criterion – #1.2	It was expected that an IT asset management tracking system was in place and contained accurate, reliable, and relevant information for decision making.
Line of Enquiry 2 – Monitoring and Maintenance Criterion #2 – IT Assets were appropriately maintained for departmental use and adequately monitored for departmental control.	
Sub-criterion – #2.1	It was expected that IT assets were adequately monitored and that monitoring results are actioned.
Sub-criterion – #2.2	It was expected that IT assets were adequately maintained.
Line of Enquiry 3 – Asset Disposal Criterion #3 – IT Asset disposals followed HC and PHAC requirements.	
Sub-criterion – #3	IT was expected that IT asset disposals followed HC and PHAC requirements.

Appendix C – Scorecard

Audit of Information Technology Asset Management at Health Canada and the Public Health Agency of Canada

Criterion	Risk Rating[1]	Risk Remaining to Program Objectives Without Implementing Recommendation	Rec #
Inventory Management and Tracking: Appropriate processes were in place for inventory management and tracking and are working as intended to ensure information is accurate, reliable, and relevant for decision making.	4	IT hardware assets are not appropriately tagged and counted, and the hardware inventory data is not accurate in SAP, thus jeopardizing the Department's ability to accurately account and properly safeguard its complete inventory of IT hardware assets.	1
	3	Policies, guidance, and standards are outdated and not carried out in accordance with current practices and systems.	2
	4	Lack of integrated planning and governance means that IT assets are not getting the attention, resources, and decisive action required. Important initiatives are at risk of not being appropriately prioritized and fulfilled, scarce resources not being effectively allocated, and cost saving opportunities being missed.	3
	5	Lack of an integrated inventory management and tracking solution for IT software assets puts the Department and Agency at risk of being in non-compliance with license agreements, presents challenges associated with manual entry and responding to vendor audits, and important information that enables effective management is not captured or readily accessible, such as purchasing documentation, software licenses, and maintenance costs. As a result, the Department and Agency are exposed to legal and financial risks.	4
	4	The lack of rigorous business process and application controls poses challenges to effectively tracking, safeguarding, monitoring, and maintaining the IT Assets. The Department and Agency are vulnerable to theft, fraud, and misuse due to data integrity concerns.	5
	4	Stakeholders are relying on inaccurate and incomplete data to manage business applications that are vital to the delivery of HC and PHAC's programs and services. As support costs are not being tracked, a key asset assessment component is missing to inform management's decision making and actions for maintaining the health of the portfolio.	6
Monitoring and Maintenance:	5	Low dollar value assets like laptops and USB keys have not been monitored, heightening the risk of lost or stolen assets that contain government or public information. It is not the value of the asset that heightens the risk, but the vulnerability of data. There have been past cases where USBs and external hard drives have gone missing or been	7

[1] Residual risk without implementing the recommendation.

Audit of Information Technology Asset Management at Health Canada and the Public Health Agency of Canada

Criterion	Risk Rating[1]	Risk Remaining to Program Objectives Without Implementing Recommendation	Rec #
IT assets are adequately monitored and maintained for departmental use.		stolen, and the reputation of the department in question has been sullied.	
	5	Business applications that are deemed critical for the delivery of essential programs and services may not be available to stakeholders if action is not taken to address those business applications that need attention, and if detailed business application maintenance plans are not developed. The Department and Agency will be increasingly unable to provide stakeholders with well-maintained, secure, and available business applications required to deliver programs and services unless steps are taken to meet or exceed the TBS minimum target, to address the aging IT concerns, and to modernize the portfolio of business applications.	8
	4	Aging hardware assets are prone to failure, may no longer be supported, nor be compatible with new business applications that are needed to achieve operational objectives without proactive maintenance. The Department and Agency's ability to make fully informed and strategic IT decisions is hindered by the lack of established performance measures and targets. As IT hardware asset disposal decisions are not being informed by full-cycle and cost-benefit analyses, IT assets are not disposed of in a timely manner, in order to gain a valuable new lease on life through the Computers for Schools program. Aging hardware also poses cybersecurity risks, as it may no longer be adequately supported and accounted for.	9
Asset Disposal: IT asset disposals followed HC and PHAC requirements.	4	Data residing in business applications may be mishandled or lost unless an appropriate authority is put in place to oversee and enforce compliance with the TB requirements governing the disposition of data. Mishandled or lost data can have legal consequences, should required data not be available for a legal hold involving ongoing litigation or for an ATIP request.	10

1	2	3	4	5
Minimal Risk	Minor Risk	Moderate Risk	Significant Risk	Major Risk