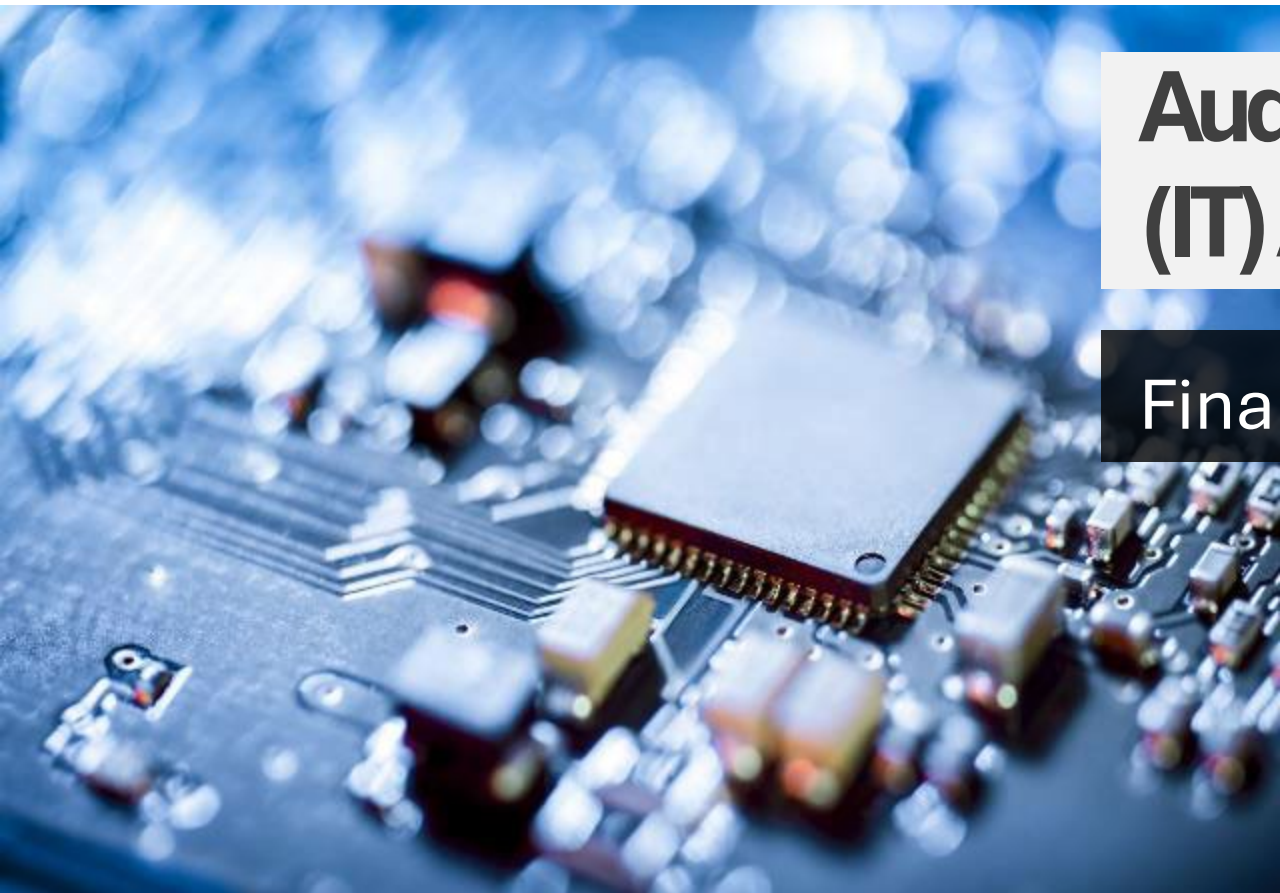




Audit of Information Technology (IT) Asset Management

Final Vetted Report

Internal Audit
November 2025



Royal Canadian Mounted Police
Gendarmerie royale du Canada

Canada

Aussi disponible en français sous le titre : Vérification de la gestion des biens de technologie de l'information (TI)

Information contained in this publication or product may be reproduced, in part or in whole by any means, for personal or public non-commercial purposes without charge or further permission, unless otherwise specified. Commercial reproduction and distribution are prohibited except with written permission from the Royal Canadian Mounted Police.

For more information, contact:
Internal Audit, Evaluation, Risk and Research
Royal Canadian Mounted Police
73 Leikin Drive
Ottawa, Ontario, Canada
K1A 0R2

www.rcmp.ca

© (2025) HIS MAJESTY THE KING IN RIGHT OF CANADA as represented by the Royal Canadian Mounted Police.

Catalogue Number: PS64-266/2026E-PDF
ISBN: 978-0-660-97829-1

Access to Information Assessment

This report has been reviewed for potentially sensitive information. Where sensitive information has been removed, [REDACTED] appears; published information is UNCLASSIFIED.



Executive Summary

p.4



About the Audit

p.6



Organizational Context

p.8



Findings

p.11



Recommendations

p.32



Appendices

p.33



Background

IT asset management (ITAM) is defined as the **continuous process** of maintaining an updated inventory of IT assets. It involves a set of policies and processes to help organizations account for all assets throughout their lifecycle.*

At the RCMP, ITAM is a **shared responsibility** between Corporate Management and Comptrollership, the Digital Program, Divisional IT Services, and Departmental Security.

ITAM plays a crucial role in the effectiveness of any organization by helping to **reduce maintenance costs, use licenses more efficiently, increase asset utilization, and better manage cybersecurity risks.**

Audit Objective & Scope

The objective of the audit was to assess whether the IT asset management control framework is adequate, and if appropriate controls are in place for IT asset management.

The audit focused primarily on the **operation and maintenance, and disposal phases** of the asset lifecycle.

The scope period was from April 1, 2022, to November 30, 2024. The audit examined desktops and laptops operating on the RCMP Office Support System (ROSS), mobile workstations (ruggedized laptops), Universal Serial Bus (USB) storage devices, and enterprise and divisional application software.

Audit Finding Themes

1. Governance

2. Inventory Management

3. Operations & Maintenance

4. Disposals

The audit found that the RCMP has an ITAM framework in place with generally understood policies. [REDACTED]

Addressing these gaps will strengthen lifecycle management and improve governance.



Key Takeaways

1. Policies are sufficient and generally understood by stakeholders, but **there are opportunities to improve** [REDACTED]
2. [REDACTED] While the IT Service Management modernization project was originally intended to provide a national solution with integrated inventory and asset management capabilities, the project has faced delays and has been rescope to exclude the inventory and asset management components. A national enterprise inventory management system would assist to improve lifecycle and financial management [REDACTED]
3. Mechanisms are in place to ensure deployed IT assets are maintained during their lifecycle but there is a [REDACTED]
4. There are **opportunities to improve the organization's disposal** practices and records management [REDACTED]

*Source: Canadian Centre for Cyber Security

The Senior Deputy Commissioner is appreciative of the audit work performed to examine the RCMP's IT asset management policies and practices and accepts the report's findings and recommendations. The audit has identified key areas requiring attention with respect to IT asset inventory tracking, the usage of USB storage devices and IT asset disposal. A comprehensive management action plan (MAP) has been developed to address the report's recommendations. Implementation of this MAP will help the RCMP to, among other things, improve IT asset inventory tracking, the proper and secure use of USB storage devices and proper and secure IT asset disposal. It will also help to demonstrate the RCMP's commitment to addressing the issues raised by the Mass Casualty Commission as they pertain to IT asset management.

The achievement of the key objectives and planned actions outlined in the MAP will be contingent upon the receipt of resources to address the recommendations. Without additional resources, the Digital Program will not have the capacity necessary to fully implement the MAP.

Bryan Larkin
Senior Deputy Commissioner

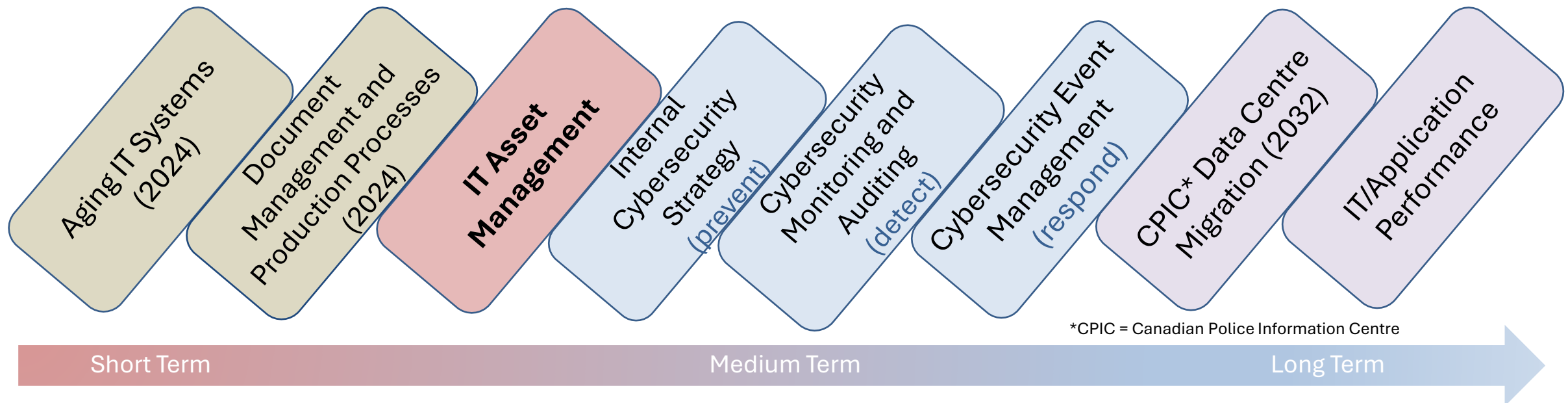
The Chief Financial Officer acknowledges the audit team's comprehensive examination and recommendations regarding RCMP's current IT asset management practices. This audit highlights the need for stronger alignment for the management of IT assets across the organization with a focus on organizational oversight, consistent tracking and disposal processes. These recommendations will serve as guiding principles to modernize and align the RCMP's practices.

Samantha Hazen
RCMP Chief Financial Officer

Audit Background

In 2023, Internal Audit conducted a Targeted Information Management/Information Technology (IM/IT) and Information Security Planning Study to assess the risk environment related to the RCMP's IM/IT universe. The result was a 5-year workplan for a suite of Internal Audit engagements with a specific focus on IM/IT and Information Security. To date, two audits have been completed with the **Audit of IT Asset Management** being the third in this series.

Figure 1 – Suite of Internal Audit's IM/IT and Information Security Engagements



Audit Objective

The objective of this audit was to assess whether the IT asset management control framework is adequate, and if appropriate controls are in place for IT asset management (See **Appendix A** for audit criteria).

Audit Scope

The scope of the audit focused on IT asset management governance, processes and activities, IT hardware and software assets, tools, business applications and disposal processes. The audit scope covered processes and activities from April 1, 2022, to November 30, 2024. The scope **included end user desktop and laptop computers operating on the RCMP Office Support System (ROSS), mobile workstations (ruggedized laptops), Universal Serial Bus (USB) storage devices, and Enterprise and divisional application software.** The audit scope **excluded non-enterprise managed devices, IT assets operating in the RCMP Classified Environment, and hardware owned and managed by Shared Services Canada.**

Methodology

The audit was conducted between September 2024 and July 2025. The audit team employed various techniques including interviews, document review, file testing, site visits and benchmarking. A sample of IT software assets was selected to assess general controls for license tracking and warranties. Benchmarking was performed by comparing observations from audits carried out by other government organizations related to ITAM. (See **Appendix C** for details on benchmarking methodology).

Divisions and Detachments/Units selected for audit testing

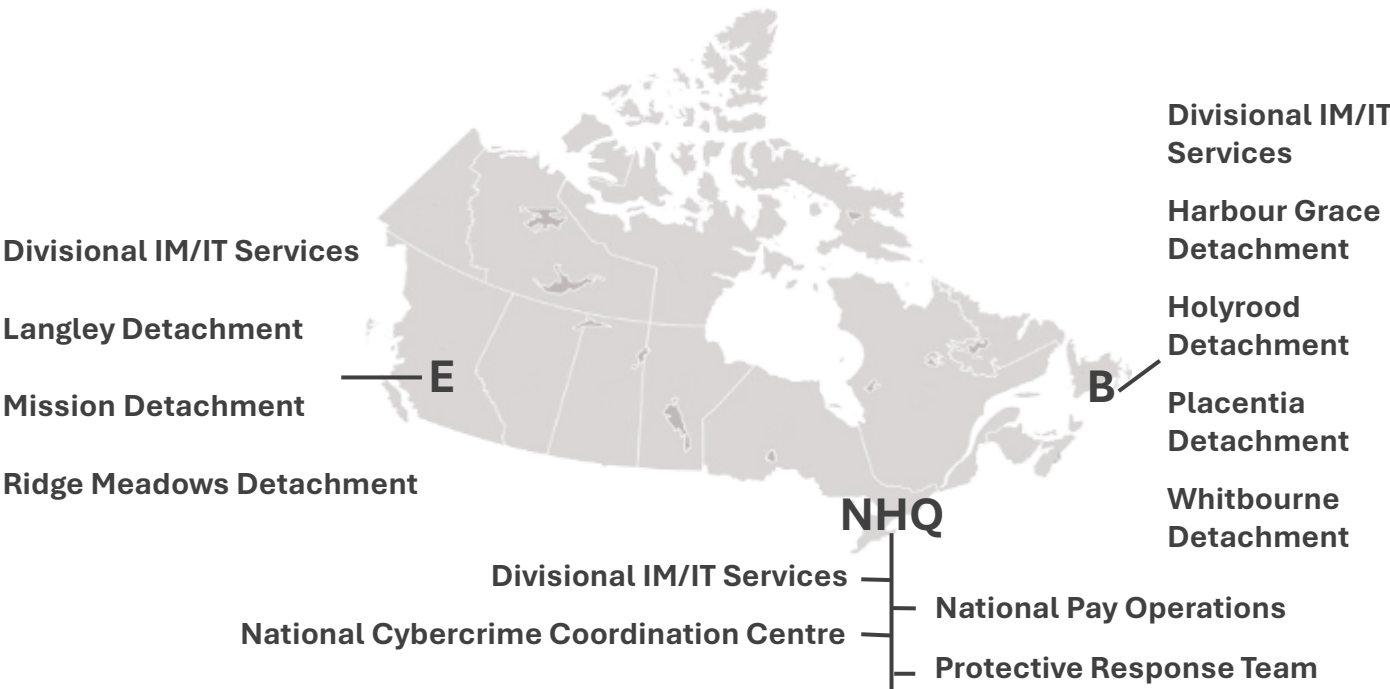


Table 1: Sample Selection per Division and Asset Type

Division	Desktop	Laptop	MWS*	Total
E	18	18	15	51
B	20	23	6	49
NHQ	12	28	11	51
Total	50	69	32	151

*MWS = Mobile workstation



Statement of Conformance

The audit engagement conforms to applicable standards in the Institute of Internal Auditor’s International Professional Practices Framework and the Treasury Board of Canada Directive on Internal Audit, as supported by the results of the quality assurance and improvement program

Horizontal IM/IT Risks impacting the RCMP

Based on Internal Audit's recent IM/IT engagements, several horizontal observations related to IM/IT risks at the RCMP have emerged:

- The organization has known **challenges with IM/IT governance and capacity**
- The organization's ability to address these issues is made more difficult due to its **decentralized nature and competing organizational priorities**
- These IM/IT challenges **can prevent the RCMP from achieving its modernization goals**

Business lines have been working on addressing these risks by implementing the Management Action Plans resulting from the audit recommendations made as part of these engagements.



IT Asset Management Roles and Responsibilities

As per policy, accountability for IT asset management is a shared responsibility between Corporate Management and Comptrollership (CM&C) and the Digital Program:

- Chief Financial Officer is accountable for all departmental assets including IT assets
- Chief Digital Officer is responsible for IT service management
- Divisional IM/IT Officers (DIOs) are responsible for IT asset management
- Chief Security Officer is responsible for IT security governance

Procurement, Materiel and Asset Management Branch

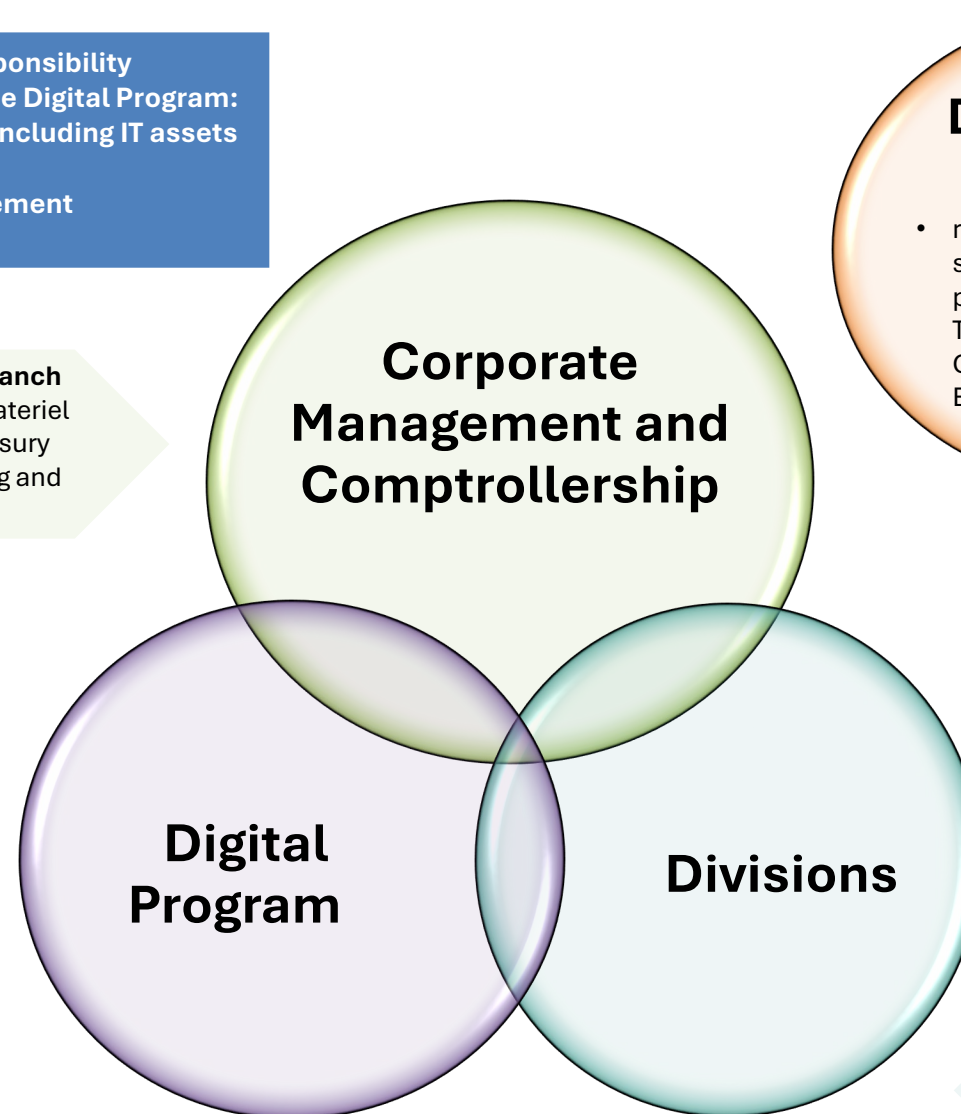
- responsible for establishing and maintaining a materiel management framework in accordance with Treasury Board (TB) policy that includes oversight, planning and reporting mechanisms

Cyber Security, Operations and Platform Support Branch

- responsible for providing IT support including managing hardware and software standards for workplace devices, and IT service management (ITSM)

Digital Strategy, Governance and Program Support Branch

- responsible for establishing procurement vehicles through which IT assets are acquired



Departmental Security

- responsible for establishing IT security governance and policies in accordance with TB policies and Communication Security Establishment's guidance

Commanding Officers

- responsible for overseeing divisions' physical, financial and human resources

Divisional IM/IT Officers (DIOs)

- responsible for the planning, acquisition, operation, maintenance and disposal of IT assets in accordance with RCMP policies, procedures and guidance

Units and Employees

- responsible for the stewardship of IT assets assigned to them

Divisional IT Asset Management Service Delivery Models

The three divisions included in the audit were structured differently, each employing varied service delivery models to perform similar ITAM-related activities.



E Division

- End-to-end asset lifecycle managed by Divisional IM/IT Services (except for USBs)
- Divisional IM/IT Services controls IT Asset Cost Element Groups
- Provincial detachments are served by Local Area Network (LAN) Administrators [REDACTED]
- Municipal detachments have onsite LAN Administrators [REDACTED]
- Asset tracking is a shared responsibility between the Units and Divisional IM/IT Services

B Division

- End-to-end asset lifecycle managed by Divisional IM/IT Services (except for USBs)
- Divisional IM/IT Services controls IT Asset Cost Element Groups
- LAN Administrators generally not co-located at detachments
- Centralized asset tracking and evergreening

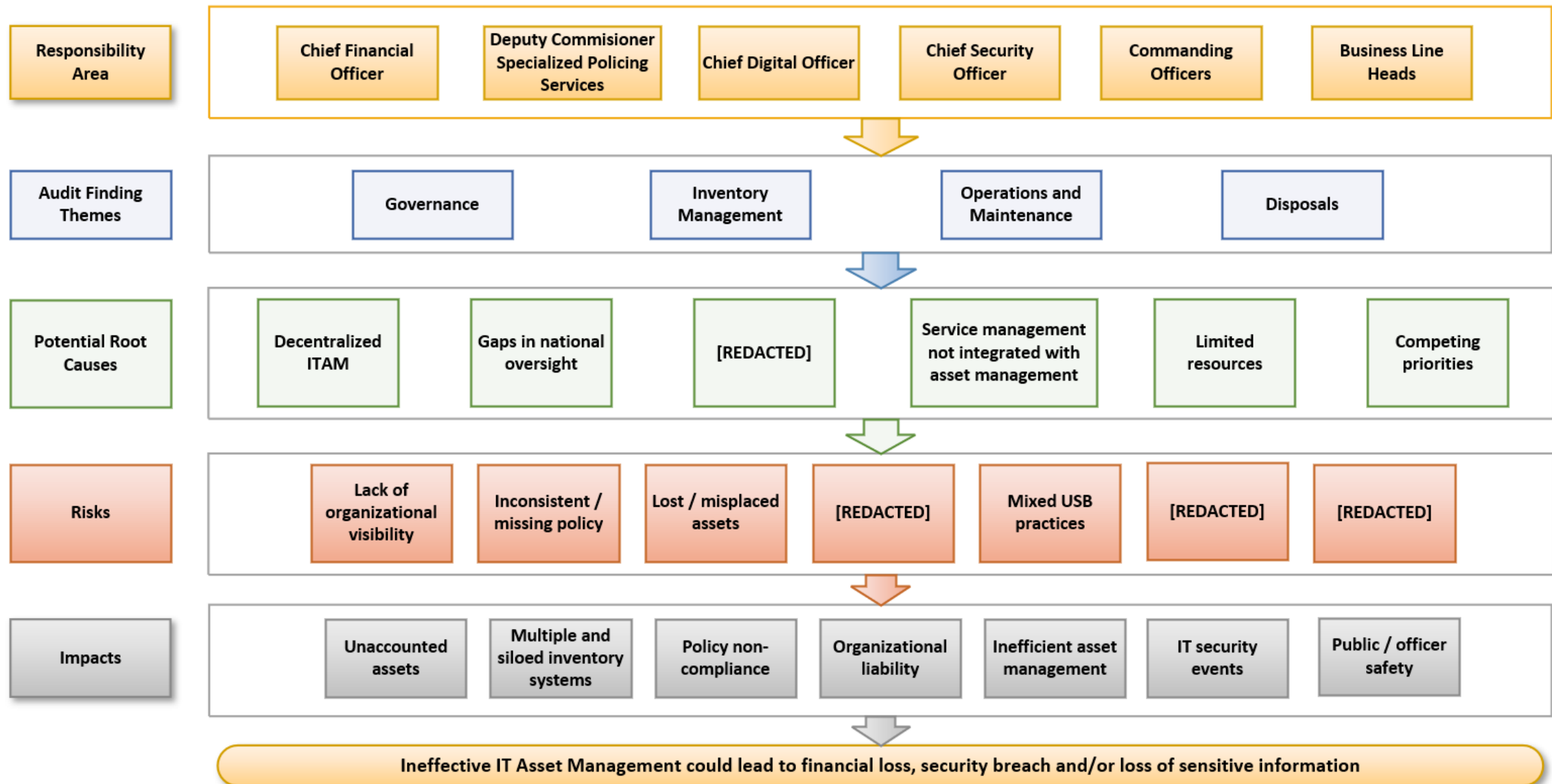
NHQ Division

- Transition to new model (April 2025)
 - Old model:**
 - Division IM/IT Services responsible for deployment and disposal of IT assets (except USBs); and supports procurement
 - Units controlled IT Asset Cost Element Groups. Units responsible for procurement (through Divisional IM/IT Services), evergreening and asset tracking
 - New model:**
 - Centralized asset tracking and evergreening
 - Division IM/IT Services controls IT Asset Cost Element Groups

*LAN Administrators are responsible for managing and maintaining networks within a geographical area

Findings: Summary of Issues and Impacts

Unclassified



Finding #1: There are opportunities to improve organizational governance and oversight surrounding the management of some IT assets and related processes

Effective governance is important in mitigating risks and maintaining control over IT assets. It encompasses the assignment of roles, the implementation of policies, and the continuous monitoring of asset-related activities. The audit assessed whether governance practices provided adequate direction and oversight to safeguard assets, promote compliance, and support informed decision-making throughout the asset lifecycle.

Roles and responsibilities are generally understood and documented

- Roles and responsibilities for ITAM are defined and documented through TB policies and RCMP manuals; **the audit found that individuals involved in ITAM generally understood their roles and responsibilities**
 - This includes Departmental Security in their role of establishing security governance
- However, **competing priorities between the Digital Program and CM&C** have led to siloed oversight of IT assets:
 - From a CM&C perspective, IT asset tracking is focused on accountability, stewardship and financial reporting (i.e. Assessment & Planning, and Acquisition phases of the asset lifecycle)
 - From a Digital Program perspective, IT asset tracking is focused on lifecycle management of the asset and ensuring employees have functioning IT tools
 - [REDACTED]



While RCMP policies are in place (i.e. Asset Management Manual - part 1) and define roles and responsibilities, the manual was last updated in 2008 and needs revisions to align with the current organizational structure. At the time of the audit, work was underway to update the manual and supporting guidance documents. 

Policies and procedures in place to support ITAM processes are generally sufficient

- At a national level, the audit found that the **policies and manuals in place adequately provided a framework and guidelines** to support strategic decision making
 - Security manuals establish requirements for the proper use of IT assets
- However, **gaps existed at the divisional level** when operationalizing policy requirements and documenting procedures related to national policies
 - [REDACTED]

Equity, Diversity and Inclusion, Gender Based Analysis Plus, Official Languages and Accessibility

Policy centres noted that the best opportunity to integrate considerations related to their areas of expertise is at the needs assessment phase of the asset lifecycle. However, for the IT assets included in the audit, none of the policy centres had been engaged in the needs assessments of these assets. It was noted that the policy centres had no concerns related to these IT assets at the time of the audit and that the Digital Program was best positioned to review assets in consideration of policy requirements.



Oversight and monitoring activities are established for key IT assets

- At the organizational level, the Investment Oversight and Prioritization Committee (IOPC) and the Committee on Digital Investments (CODI) are responsible for reviewing and approving new proposals for digital investments in the context of strategic investment planning.
- At a national level, there is no dedicated senior-level committee specifically responsible for IT asset management. However, the following national oversight activities are in place:
 - The Digital Program, in consultation with the divisions, provides parameters for asset procurement
 - National **maintenance plans are in place**, with User Computing Devices Section (UCDS) deploying updates and security patches
 - There are monthly teleconferences with divisional personnel to ensure their needs are being met
 - The Digital Program has leveraged **system-driven active monitoring** to ensure laptops, desktops and MWS on the RCMP network are receiving the latest software updates and security patches; **mechanisms are in place to address outliers** in coordination with Divisional IM/IT Services
- Divisionally, IT asset management is led by the divisions' respective DIOs in consultation with the Divisional Executive Committee (except for NHQ)
 - Divisional interviewees identified that the **evergreening schedule** for laptops, desktops, and MWS **prompts monitoring** allowing for predictability and planning for funding
 - Physical monitoring of deployed assets is decentralized (i.e. at the unit level)
- **The management and monitoring of USB storage devices is decentralized** (Additional related findings are discussed on slides 18 & 19)

ITAM training is primarily on-the-job training due to the varying service delivery models across the RCMP

Interviewees did not have any major concerns with current training practices noting that ITAM is less technical than other areas of IM/IT



Why it matters

- While decentralized IT asset management can provide flexibility and responsiveness, the audit findings highlight the need for **strengthened governance** to address key risks:
 - **Policy compliance** – inconsistent governance across asset classes may result in incomplete audit trails or **misalignment with organizational policies and priorities**
 - **Outdated policies** – can result in confusion over roles and responsibilities and weaken the framework supporting the overall management of IT assets
 - [REDACTED]
 - [REDACTED]
- In response to the audits of Aging IT Systems and Document Management & Production Processes, Specialized Policing Services and the Digital Program are undertaking concrete actions to strengthen governance in the areas of aging IT systems, technical debt and information management. Although distinct from IT asset management, improvement in the governance of these areas could also help strengthen the overall stewardship of the organization's IM/IT resources.



Benchmarking – How are others doing?

A review of audit reports from various other government organizations noted the following strengths and weaknesses in ITAM governance

Strengths

- Most departments had formal governance structures and policies in place
- Roles and responsibilities were generally defined at a high level

Weaknesses

- Lack of centralized oversight or enterprise-wide coordination
- Fragmented accountabilities across units



Finding #2: [REDACTED]

IT asset tracking and inventory management play an important role in ensuring the availability, security, and accountability of technology assets throughout their lifecycle. The audit examined whether current practices effectively supported the maintenance of complete and accurate asset records to support effective oversight of assets throughout their lifecycle.

Various tools are in place to track and monitor IT assets at the divisional and unit level, [REDACTED]

[REDACTED]

- The audit found that IT asset **inventory tracking varied across divisions and units**:
 - E Division uses Service Desk Express at the divisional level and spreadsheets at the detachment level
 - B Division has one centrally managed spreadsheet with no detachment level tracking occurring
 - NHQ Division tracking processes are in transition - prior to April 2025, tracking was done at the unit level; post April 2025, centralized tracking at Divisional IM/IT Services
 - [REDACTED]
- One key tool in place **to assist with inventory tracking was the use of asset tags**
 - Asset tags are affixed to the asset and are labelled with pertinent information
- [REDACTED]
- [REDACTED]
 - As part of its new service delivery model, NHQ Division recently started assigning assets (e.g. laptops) to individuals rather than positions/units to facilitate asset tracking

Various asset tags in use

[REDACTED]	[REDACTED]
[REDACTED]	
[REDACTED]	

Audit testing indicated generally strong compliance with IT asset management controls, [REDACTED]



Physical Location

- **Test:** assets sampled from records should be physically located at the Detachment/unit
- **Result: 98% compliance;** 78 of the 80* assets tested for “book-to-shelf” were physically located
- **Gap:** Two assets were unaccounted for (Management was apprised of the situation, and it was confirmed that both assets were “inactive” and did not have ROSS connectivity.)

**The sample of 151 assets was divided to test 80 assets for “book-to-shelf” and 71 assets for “shelf-to-book”*

The audit found 100% compliance for “shelf-to-book”



Asset Tag Existence

- **Test:** sampled assets are labelled with a tag containing relevant identifying information
- **Result: 97% compliance;** 142 of the 146** assets tested had an asset tag with identifying information on it
- **Gap:** the four assets missing asset tags were MWS
- Three of these four assets had an alternative label which indicated the asset’s workstation identification WSID #

***Five assets were removed because the audit team was unable to physically observe the asset, therefore, the asset tags were not assessed for existence and legibility (two assets were unaccounted for; three assets were offsite)*



Accuracy of Records

- **Test:** information contained on the asset tag should be accurate, matching Divisional records and unit level records (if applicable)
- **Result: 83% compliance;** 114 of the 138*** assets tested had discrepancies between the asset tag and divisional/unit records
- **Gap:** 24 assets were found to have discrepancies between the information on the asset tag and either the local and/or Divisional records (location of the asset, make/model, warranty dates)

**** 13 assets were removed because those assets were shared assets between units, and the sampled unit did not have access to the asset records*



Asset Tag Legibility

- **Test:** information contained on the asset tag should be legible
- **Result: 93% compliance;** 136 of the 146** assets tested had a tag with fully legible information
- **Gap:** Nine tags were partially legible; one was fully illegible

[REDACTED]



Approved Hardware

- **Test:** sampled assets are RCMP approved
- **Result: 100% compliance;** All 151 hardware assets were found to be on the RCMP approved hardware list

[REDACTED]

[REDACTED]



- As per Departmental Security standards, **authorized individuals may have an operational requirement to utilize USB storage devices** for transferring large quantities of information to and from an RCMP ROSS workstation or network resource to carry out their duties
 - Each USB device is required to have a register for logging its location and details surrounding all data transfers (E.g. Individual performing transfer, date and time of transfer, list of files transferred, etc.)
- [REDACTED]
- [REDACTED]

USB storage device practices do not align with policy requirements

The audit team interviewed 36 employees across three divisions to observe USB practices

Unit-issued USBs

- 17 out 36 employees interviewed had a unit-issued USB
- Unit-issued USBs were used for a variety of purposes including court disclosures, transferring documents, storing video and surveillance data, and storing other data as part of an investigation
- [REDACTED]

Personal USBs

- [REDACTED]
- [REDACTED]
- [REDACTED]

Division	Unit-issued USB	Encrypted	[REDACTED]
E	11	10	[REDACTED]
B	2	1	[REDACTED]
NHQ	4	2	[REDACTED]
Total	17	13	[REDACTED]

Division	Personal-issued USB	Encrypted	[REDACTED]
E	4	4	[REDACTED]
B	5	1	[REDACTED]
NHQ	1	0	[REDACTED]
Total	10	5	[REDACTED]

USB Risks



- [REDACTED]
- [REDACTED]



[REDACTED]

Recent Initiatives

USB Bounty Program

- In July 2025, **E Division** initiated the **USB Bounty Program** to collect and dispose of unauthorized USB storage devices; and to supply and distribute USBs to authorized users that will be encrypted and inventoried
- The USB Bounty Program also aims to educate and raise awareness on approved alternatives (e.g. OneDrive/MS Teams/M365, Secure File Transfer, Liquid Files) and provide education and awareness on general use and user obligations related to USB storage devices

Security Reporting

- In July 2025, **Departmental Security** released a **new Security Event Reporting Program icon on all RCMP employees' desktops** to facilitate security event reporting.



USB Encryption Software

- In May 2025, **K Division** introduced a new USB Encryption Software – [REDACTED]
- This software is intended to help the user encrypt USBs using BitLocker and streamline the monitoring of USBs

Management of IT software assets

Software license tracking practices vary across divisions and lacks centralized oversight for non-enterprise licenses. [REDACTED]

Enterprise Managed Software

- Common enterprise level software (e.g. Microsoft, Adobe, Antidote) is centrally managed by the Digital Program
- Audit testing confirmed **that system controls exist to identify software assets installed on specific computing devices.** This allows for monitoring of approved software and whether the latest patches have been installed

Non-Enterprise Software Tracking

E Division:

- **Software licenses are centrally tracked as assets and linked to hardware**
- Expiry tracking for non-enterprise software is the responsibility of work units, increasing the risk of inconsistent monitoring

B Division:

- **Division maintains a central record but relies on detachments to proactively send purchase orders to ensure records are complete**
- [REDACTED]

NHQ Division:

- **No formal mechanisms are in place to track software licenses at the divisional level.** This responsibility is left to individual work units to maintain the inventory, proof of purchase, etc
- [REDACTED]



ITSM modernization project will offer a national solution for service management without the inclusion of inventory/asset management capabilities



- Most managers interviewed noted that a **major improvement required from an IT asset management perspective would be the implementation of an enterprise information system** which could track all IT assets throughout the lifecycle and be used by all Divisions
- The Digital Program is currently undertaking an ITSM modernization project, to **replace the existing IT service ticketing system - Service Desk Manager (SDM) - with IT Services and Asset Management System (iTSAMS)**
- iTSAMS is intended to modernize and transform service delivery by automating processes, reducing risk, and preventing points of failure during the delivery of IT service operations
- During the audit, management indicated that iTSAMS would be deployed with an integrated asset tracking module. Due to funding pressures, the project has since been rescoped to deliver only the service management functionality, [REDACTED]
- Phase 1 of the implementation, originally planned for January 2025, was delayed and **as of July 2025, iTSAMS has not been rolled out.** Training for its future use is underway for individuals within the Digital Program, Divisional IM/IT, and support groups in program areas with IT service management roles

Why it matters

- Keeping an accurate and up-to-date inventory of IT assets is important to any organization as it enhances:
 - [REDACTED]
 - **IT Operations – promotes effective and efficient asset lifecycle management** by minimizing downtime, facilitating IT support, ensuring policy compliance and avoiding duplicate/unnecessary purchases
 - **Strategic Planning – provides adequate data for IT planning and investment decisions** (e.g. digital transformation)
- [REDACTED]



Benchmarking – How are others doing?

A review of audit reports from various other government organizations noted the following strengths and weaknesses related to inventory tracking

Strengths

- Most departments used inventory tools such as System Center Configuration Manager and Axios Assyst to track assets
- Some departments had begun integrating hardware and software inventories

Weaknesses

- Inventories were often incomplete, outdated or not reconciled with physical assets
- Lack of real-time tracking and automation
- Poor integration between procurement, inventory and disposal systems



Finding #3: Mechanisms are in place to ensure deployed hardware assets are maintained during their lifecycle

IT asset operations and maintenance are critical stages of the lifecycle, ensuring assets remain secure, functional and cost-effective. The audit assessed whether timely updates and security patches were applied, evergreening standards were in place and asset replacements were carried out in line with policies.

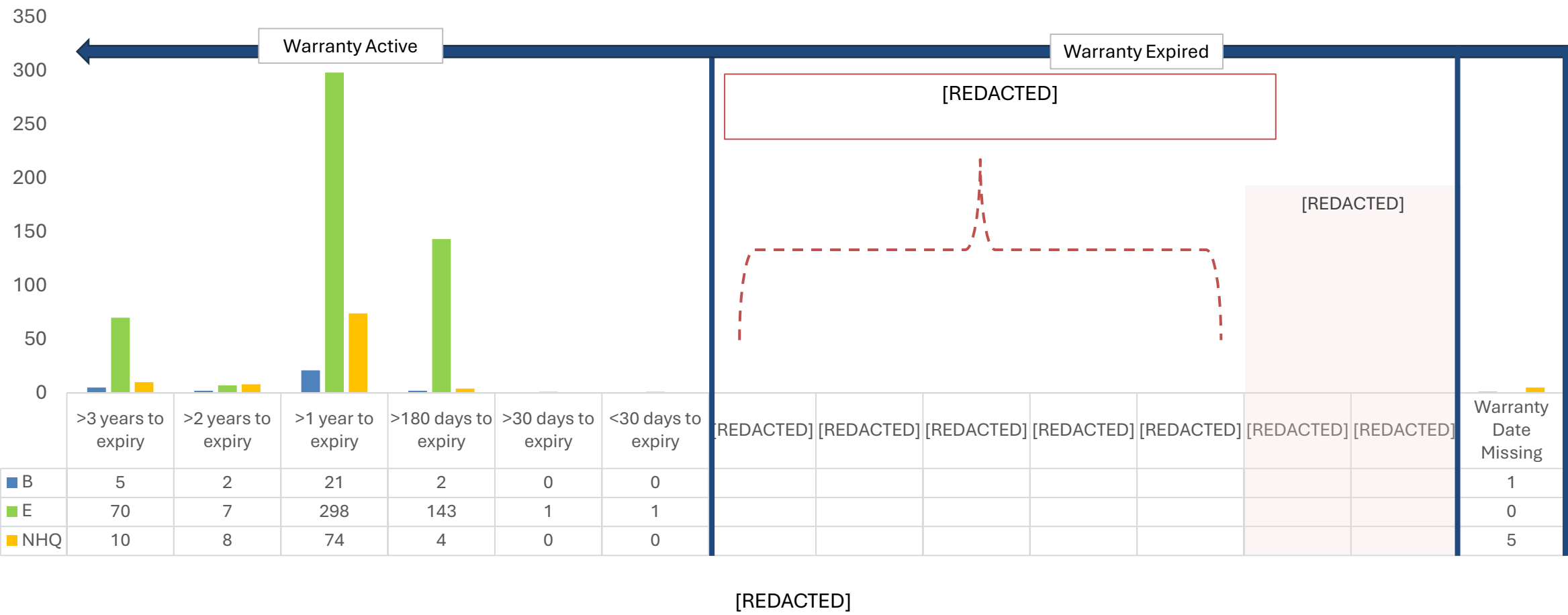
Although national IT asset maintenance and divisional evergreening are in place, there are opportunities to improve organizational visibility to help support investment decisions for hardware and related warranties

- The Digital Program has national maintenance plans in place for IT assets
 - Periodic **system monitoring exists to detect outdated and/or unpatched computers**; the Security Operations Centre and/or UCDS will notify Divisional IM/IT managers to locate, upgrade or replace these vulnerable computers
 - Some software updates require end user intervention (e.g. Software Center) while critical updates are automatically deployed nationally by UCDS
 - Service requests are made through SDM and dispatched to Divisional IM/IT Services (and/or LAN Administrator); repairs can either be software related, or hardware related
- Sampled **IT assets had similar evergreening standards in place** for all three divisions:
 - Desktops and laptops are procured with a 3-year manufacturing warranty
 - MWS are procured with a 5-year manufacturing warranty
 - Divisional IM/IT Services will provide an additional 2-years of IT support for these IT assets (i.e. post warranty period)
- While evergreening standards were similar, the audit noted variation in their implementation among Divisions possibly leading to uneven risk exposure and technology gaps
- In **E Division**, the yearly IT Plan serves as a **basis for forecasting**. While a **formal evergreening process is still evolving**, IT assets are proactively procured in bulk and allocated based on demand. Efforts are underway to enhance forecasting capabilities and ensure inventory levels align with divisional needs
- In **B Division**, asset warranty expirations currently inform evergreening efforts, with future replacements planned to ensure employees are equipped with up-to-date equipment.
- As **NHQ Division** is transitioning to a centralized service delivery model, the evergreening process will be centralized to reduce unnecessary spending and/or evergreening prematurely; however, a **standardized process was not yet in place** at the time of the audit
 - NHQ Division is also considering the redistribution of used assets (within an acceptable age range) among employees allowing spares to be held centrally and deployed when needed

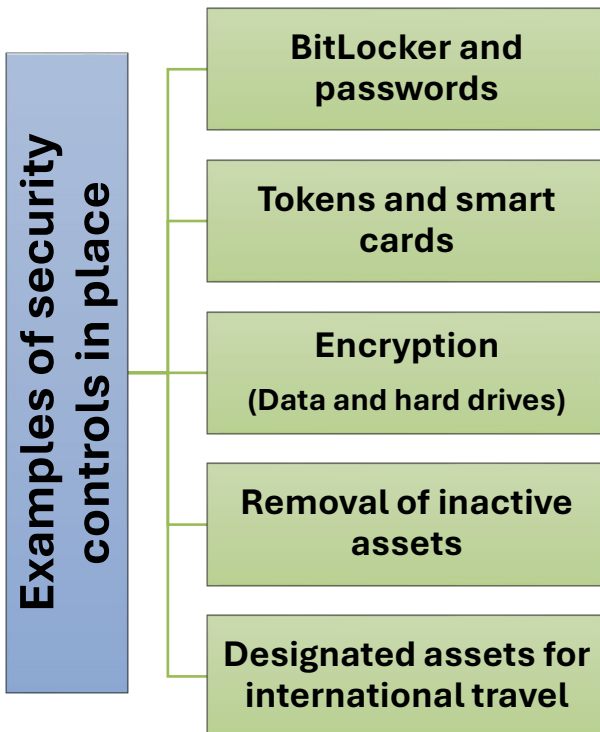


Asset Aging and Warranty Status

Graph 1: Divisional Comparison of IT Assets' Age as of May 2025 (Full Detachment/Unit Inventory)



Security mechanisms are generally in place to protect IT assets from being breached or misused



- The audit team obtained evidence from UCDS to substantiate that the Digital Program **monitors IT assets that have not received the latest security patches**; for example, they recently tasked Divisional IM/IT Services to locate each of these assets in the divisions and to either replace or upgrade them
 - UCDS also provided proof of Operating Systems patches that are currently underway
 - Shared Services Canada is responsible for delivering these specific patches while UCDS coordinates and approves them
 - [REDACTED]
 - As MWSs are not always connected to the network, they have their security patches uploaded manually; MWSs are updated based on a schedule and tracked at the divisional level
- [REDACTED]
- The audit found that all three divisions stored their IT assets in accordance with the Departmental Security's storage requirements
 - Interviewees had no concerns over the physical storage of assets, however, **having additional storage space was often identified as something that would be beneficial**



Why it matters

- **Strong IT maintenance and evergreening practices help ensure that assets remain reliable, secure, and within warranty coverage throughout their lifecycle.** However, key organizational risks remain:
 - [REDACTED]
 - **Cost Optimization** – decentralized evergreening may lead to inconsistent refresh cycles, potential over- or under-investment in assets, and missed opportunities to optimize lifecycle value
 - [REDACTED]



Benchmarking – How are others doing?

A review of audit reports from various other government organizations noted the following strengths and weaknesses related to IT asset maintenance and evergreening.

Strengths

- Some departments had long-term IT asset plans or refresh strategies

Weaknesses

- Aging IT hardware was not consistently monitored or replaced, increasing operational and security risks
- Low-value assets were often excluded from performance monitoring
- Limited use of performance metrics to guide refresh cycles



Finding #4: There are opportunities to improve the organization's disposal practices

IT asset disposal is a key part of the lifecycle, helping protect data, reduce costs, and support reuse. The audit **assessed whether disposal practices met key obligations: safeguarding data, maintaining suitable disposal records**, and complying with the TB Policy requirement to offer surplus IT hardware to the Computers for Schools (CFS) program

While there is one national IT system to record IT asset disposals, record-keeping could be improved to strengthen accountability

- In 2022, the RCMP's Disposal Report Online Form (Form 1989) was discontinued and replaced with the Asset Divestment Request (ADR), an electronic form in TEAM. As of July 26, 2022, **all requests and subsequent approvals for asset disposal are required to be completed via ADRs**
- This process was implemented to **streamline requests and approvals** of all assets for disposal while also **improving the monitoring of assets** at the national level
- Audit testing of disposal transactions noted some areas for improvement with respect to retaining supporting documentation:
 - [REDACTED]

[REDACTED]

Disposal process differs across Divisions and there is limited oversight and monitoring

- E, B and NHQ Divisions were all in compliance with TB Policy by offering end-of-life IT assets to Computers for Schools (CFS) for first right of refusal
- Hard drive sanitization procedures differed between the three Divisions
 - E Division Detachments visited had removed the hard drives from computers to be donated and [REDACTED] awaiting further direction from EHQ IM/IT
 - B Division and E Division HQ used [REDACTED] to sanitize hard drives prior to donating IT assets
 - NHQ Division removed hard drives from IT assets prior to donating; [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Security controls such as BitLocker and full disk encryption mitigate disposal risk. These prevent unauthorized access to data in cases of loss, theft, or incomplete sanitization of end-of-life hardware.

[REDACTED]

Findings: Disposals

Summary of audit observations for IT asset disposals

Criteria	E Division	B Division	NHQ
Disposal Method	[REDACTED]	[REDACTED]	[REDACTED]
Drive Sanitization	[REDACTED]	[REDACTED]	[REDACTED]
Physical Security	[REDACTED]	[REDACTED]	[REDACTED]
Approval	[REDACTED]	[REDACTED]	[REDACTED]
Record Keeping	[REDACTED]	[REDACTED]	[REDACTED]

Why it matters

- Having a consistent disposal process, supported by adequate records of disposal and periodic verifications, is key to any organization to enhance:
 - **Security** – data wiping or physical destruction reduce the risk of security breaches
 - **IT Operations** – assists in the tracking of IT assets and reducing the risk of unaccounted assets
 - **Oversight** – provides a paper trail to demonstrate compliance with policies and procedures
- [REDACTED]

[REDACTED]

[REDACTED]

Benchmarking - How are others doing?

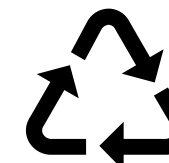
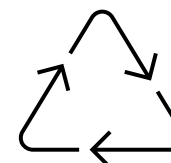
A review of audit reports from various other government organizations noted the following strengths and weaknesses related to IT asset disposal.

Strengths

- Disposal processes in place often aligned with policies and standards
- Some departments followed secure disposal protocols for sensitive equipment

Weaknesses

- Disposal activities were inconsistently documented or tracked
- Weak oversight of data sanitization and environmental compliance
- Lost or stolen assets did not always have sufficient information or follow-ups



The audit found that there are opportunities to improve the IT asset management framework and controls in place, specifically:

1. Policies are sufficient and generally understood by stakeholders, but **there are opportunities to improve organizational oversight surrounding the management of some IT assets** and related processes [REDACTED]



2. [REDACTED] While the IT Service Management modernization project was originally intended to provide a national solution with integrated inventory and asset management capabilities, the project has faced delays and has been rescoped to exclude the inventory and asset management components. A national enterprise inventory management system would assist to improve lifecycle and financial management [REDACTED]



3. Mechanisms are in place to ensure deployed IT assets are maintained during their lifecycle but there is a [REDACTED]



4. There are **opportunities to improve the organization's disposal practices, related monitoring and records management** [REDACTED]

Addressing these challenges will be required in achieving a mature, integrated ITAM framework that supports operational efficiency, financial stewardship, and risk mitigation across the enterprise

To **support effective organizational governance and oversight**, the Senior Deputy Commissioner, in collaboration with the Chief Financial Officer and Commanding Officers, should:

Recommendation	Benefits
1. [REDACTED] pursuing efforts to identify and implement a solution that enables organization-wide integration of IT service management and IT asset inventory tracking. In the interim, existing processes should be strengthened [REDACTED]	✓ Increase efficiency of the management of IT assets ✓ [REDACTED] ✓ Help inform IT asset investment decisions
2. Address gaps related to the usage of USB storage devices by leveraging system controls where possible, continuing to promote secure alternative file transfer tools, enhancing employee culture and awareness of related policies, and establishing processes to monitor and enforce compliance.	✓ [REDACTED] ✓ Manage inherent risks related to the usage of USB storage devices
3. Address gaps in IT asset disposals to ensure timely and complete disposals of IT assets in accordance with relevant policies, and are supported by appropriate documentation and periodic monitoring.	✓ Improve the organization’s existing IT asset disposal practices ✓ [REDACTED] ✓ Reduce organizational risk

Audit Objective:

The objective of this audit was to assess whether the IT asset management control framework is adequate, and if appropriate controls are in place for IT asset management

Criteria 1

- An effective governance to oversee IT Asset Management is in place across the RCMP

Criteria 2

- The RCMP maintains an accurate and up-to-date inventory of its assets

Criteria 3

- Mechanisms are in place to ensure deployed IT assets are effectively maintained during their lifecycle.

Criteria 4

- The RCMP is effectively managing risks related to the disposal of IT assets

Audit Recommendation	Area of Responsibility	Planned Action	Diary Date
To support effective organizational governance and oversight, the Senior Deputy Commissioner, in collaboration with the Chief Financial Officer and Commanding Officers, should: 1. [REDACTED] pursuing efforts to identify and implement a solution that enables organization-wide integration of IT service management and IT asset inventory tracking. In the interim, existing processes should be strengthened [REDACTED]	Director General, Cyber Security, Operations & Platform Support, with support from CM&C	Agree. The RCMP continues with their migration from the current SAP ERP (Corporate system) which is reaching end of life, to SAP's new offering for fiscal year 2027, which is planned to go live in April/May 2027. During this time work will be done to pilot a small segment of the IM/IT assets to gradually build up requirements allowing for a national solution to start onboarding for April of 2028. For example, discussions with the Digital Program regarding the pilot of mobile assets – cell phones – have begun (dates and milestones TBD). In addition, Corporate Management is currently working with E Division to onboard IM/IT equipment within SAP. To help inform the development of the new SAP system, the Digital Program will work closely with Corporate Management & Comptrollership to identify business requirements associated with IT asset tracking. In addition, the Digital Program will work with Divisional Informatics Officers to nationalize and streamline existing processes while validating data to support a future data migration. In the interim the Digital Program will continue to monitor IT assets through existing yearly reporting to the DP on IT spending and IT procurement. As well, the host-based sensors deployed by the Cyber Security Operations Centre (CSOC) will assist in identifying active assets and their status as long as they are active on the RCMP infrastructure. Furthermore, the DIOs will continue to track their IT assets through existing processes. The pursuit of an interim enterprise software solution tool will take too long and duplicate what the modernized SAP system will provide.	April 2028

Audit Recommendation	Area of Responsibility	Planned Action	Diary Date
2. Address gaps related to the usage of USB storage devices by leveraging system controls where possible, continuing to promote secure alternative file transfer tools, enhancing employee culture and awareness of related policies, and establishing processes to monitor and enforce compliance.	1. USB bounty: DG, Cyber Security, Operations and Platforms Support 2. Shared drive and file shares: DG, Analytics, Data and Information Management (ADIM)	1. USB bounty: The RCMP Digital Program is implementing a new encryption solution [REDACTED] for USB media on managed ROSS devices. This initiative will force all RCMP users to easily encrypt USB devices containing RCMP information, significantly reducing the risk of data loss or unauthorized access. Several divisions also contributed through USB bounty programs that helped remove legacy devices from circulation. 2. Shared drive and file shares: The RCMP Digital Program is examining alternate technologies for file shares while also preparing to move the majority of its current information holdings to SharePoint Online (SPO). A project is currently underway, Digital Collaboration and Information Management (DCIM), that will set up and configure SPO with information labeling, security classification, and other meta data to enable proper information management life cycle. The SPO platform will also allow for collaboration and sharing of files across the department and with external partners and agencies as we broaden our external access connections. This will reduce the need for external devices such as USBs or external hard drives for information and data exchange with partners and stakeholders. When the DCIM project is implemented, there will be training and information management resources available for employees to understand how best to use these modern tools. Once information migration starts, information management professionals will work with business lines and divisions to organize and clean their information. They will also provide advice and guidance to support their learning of information management policies and directives as well as tools for sharing and collaborating. DCIM will start to become available in late fall 2025 and finish implementation by Q1 of the FY 2026-27. This initiative will also support the decommissioning of aging IT infrastructure across the RCMP, creating an opportunity to expedite data migration and reinforce compliance with organizational standards.	1. USB bounty: Phase 1 - November 2025; Phase 2 – January 2026 2. Shared drive and file shares: October 2026 completion

Audit Recommendation	Area of Responsibility	Planned Action	Diary Date
	3. One drive: DG, Analytics, Data and Information Management (ADIM)	3. OneDrive: OneDrive is currently available to all users in the RCMP. An initiative is underway to move all personal drive information currently housed on outdated technology to employee OneDrive. Beginning March 2025 communications were sent with links to resource materials to support employees in moving this information themselves, however a project team is also testing methods to automate the transfer of information. Additional information sessions are planned through the MS Cafes, a forum for learning about M365 products. This work is underway and expected to be completed by end of FY 2025/26.	3. One drive: March 2026
	4. SPO: DG, Analytics, Data and Information Management (ADIM)	4. SharePoint Online (SPO): As noted above, SPO is being configured and set up to become RCMP's next enterprise modern information management solution. Work is currently underway via the DCIM project and expected to be completed by Q1 of FY 2026/27. SPO will offer a fast, easy way for employees to collaborate internally and externally to the organization and manage file exchanges in a more secure and reliable way. That said, many business lines have current SPO sites that can and do facilitate sharing with partners and stakeholders. At this time, SPO is for collaboration purposes, and these sites will be reviewed and cleaned during information migration in the DCIM project.	4. SPO: Collaboration sites available now, configured IM sites April 2026
	5. Liquidfiles: DG, Digital Solutions & Systems Delivery	5. LiquidFiles: LiquidFiles began as a Pilot at the RCMP in June 2020 and was approved as an Enterprise solution in November 2024. LiquidFiles is currently the recommended enterprise application for the electronic sharing of all Protected A and Protected B transitory files with external users and for the external sharing of all large unclassified files (larger than 20 MB). The RCMP instance of LiquidFiles supports sizes up to 500 GB by default or with an exception up to 2TB in one message. LiquidFiles is also the recommended solution for internal RCMP to RCMP electronic sharing of transitory files that are larger than 250 GB.	5. Liquidfiles: Available since November 2024

Audit Recommendation	Area of Responsibility	Planned Action	Diary Date
		These very large files are not supported by the RCMP instance of OneDrive or SharePoint. We continue to promote the more secured LiquidFiles solution over the use of secure USBs. Since LiquidFiles became an RCMP Enterprise solution, the user adoption has been steadily increasing each month and currently (as of end of August 2025) there are over 4,000 RCMP users using LiquidFiles to send or request files. There is approximately 8.3TB of data uploaded each month in the system as of August 2025. Additionally, there is an opportunity to expand the current LiquidFiles licensing, enabling the RCMP to leverage this secure large file transfer solution more broadly. This would enhance data protection and directly address risks associated with USB-based data loss, as previously identified by the Office of the Privacy Commissioner.	

Audit Recommendation	Area of Responsibility	Planned Action	Diary Date
3. Address gaps in IT asset disposals to ensure timely and complete disposals of IT assets in accordance with relevant policies, and are supported by appropriate documentation and periodic monitoring.	Chief Security Officer	1. Policy Review and Update - Review the current IT asset disposal policy and procedure to ensure alignment with: - RCMP Departmental Security Policy - GC IT Security Policy and Directive on Disposal of Protected/Secret Assets - Update the policy to explicitly require: - Approved disposal methods secure data sanitization (e.g., overwrite, physical destruction) - Chain-of-custody documentation for all disposals - Approval Sign-off before disposal - Publish the updated policy on the InfoWeb and communicate it via the InfoWeb rotator. 2. Implement a Disposal Authorization Workflow - Recommend a standardized disposal request and approval process. - Implement authority for asset disposal. 3. Periodic Monitoring and Reporting - Establish periodic monitoring of disposal records to verify: - Timeliness of disposal - Completeness of documentation - Compliance with security requirements	October 2026

Approach

The internal audit team reviewed six Canadian government audit reports on IT asset management to compare strengths, gaps and recommendations across four key themes – (1) governance, (2) inventory information systems, (3) maintenance and evergreening, and (4) disposals.

The following **publicly available (open source) audit reports from Canadian government organizations** were reviewed for benchmarking purposes:

Organization	Report
Organization 1	Report 1
Organization 2	Report 2
Organization 3	Report 3
Organization 4	Report 4
Organization 5	Report 5
Organization 6	Report 6

Common Findings across Organizations

- Governance and accountability:** Most departments have frameworks in place, but roles and responsibilities are inconsistently applied.
- Inventory Management:** Incomplete, outdated, or inaccurate inventories are recurring issues, undermining asset visibility.
- Lifecycle Oversight:** Weaknesses in tracking assets from acquisition to disposal increase risk and reduce cost-effectiveness
- Cybersecurity Risk:** Poor asset tracking and aging hardware elevate exposure to security threats.
- Disposal and Decommissioning:** Disposal processes often lack documentation, oversight, or integration with security protocols.
- Performance Monitoring:** Limited use of performance metrics and reporting impairs strategic decision-making.

Strategic Risks Identified:

- Security Exposure:** Untracked or outdated devices increase breach risk
- Operational Inefficiency:** Redundant or underutilized assets inflate costs
- Compliance Gaps:** Inconsistent disposal and reporting practices
- Gaps in Visibility for Decision Making:** Lack of performance data impairs planning



ADR	Asset Divestment Request
CFS	Computers for Schools
CM&C	Corporate Management and Comptrollership
CPIC	Canadian Police Information Centre
DIO	Divisional IM/IT Officer
IM/IT	Information Management/Information Technology
IT	Information Technology
ITAM	Information Technology Asset Management
iTSAMS	IT Services and Asset Management System
ITSM	IT Service Management
LAN	Local Area Network
MWS	Mobile Workstations
NHQ	National Headquarters
RCMP	Royal Canadian Mounted Police
ROSS	RCMP Office Support System
SDM	Service Desk Manager
TEAM	Total Expenditure Asset Management
TB	Treasury Board
UCDS	User Computing Devices Section
USB	Universal Serial Bus