

Audit of Aging Information Technology (IT) Systems

Final Report

Internal Audit

January 2025



Aussi disponible en français sous le titre : Vérification sur le vieillissement des systèmes 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 and Review
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: PS64-245/2025E-PDF
ISBN: 978-0-660-75778-0

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.

Table of Contents

1	Executive Summary.....	3
2	Audit Approach.....	7
3	Organizational Context.....	10
4	Key Audit Findings.....	16
5	Case Studies.....	32
6	Conclusion.....	38
7	Appendices.....	41

1 Executive Summary

- A. Context
- B. Key Takeaways
- C. Management Response

Context

The Royal Canadian Mounted Police (RCMP) relies heavily on IT systems to deliver on its mandate to keep Canadians safe and secure. Some of these systems, though currently operational, have been in use for more than 30 years, and the extent to which they are well-suited to the current and evolving needs of the organization is unclear.

Aging IT systems rely on dated technology that is increasingly costly to support, may no longer be supported by the vendor or require expertise that is increasingly scarce. Outdated systems are also more vulnerable to cybersecurity threats, and increase the likelihood of system failures during crisis situations. Additionally, there is a risk of reduced operational delivery in remote/rural areas, untimely decision-making, and not meeting the safety and security needs of RCMP employees and the public.

The RCMP is continuously addressing aging IT risks. In 2023, the RCMP decommissioned three legacy systems – two were migrated to new modern systems, and one was no longer in use; additionally, 11 servers were decommissioned as a result of these decommissioned systems and/or infrastructure evergreening.

Audit Objective

To assess the adequacy and effectiveness of the RCMP's management and modernization of its aging IT systems

Audit Themes

The audit findings are grouped into the following themes:

1. Information Management/IT (IM/IT) Governance
2. Management of IT Systems
3. Management of Technical Debt

Audit Scope

- Fiscal years 2018-19 to 2022-23
- Inventory of enterprise-wide, aging IT systems
- Governance structures
- IT investment plans
- Key modernization projects
- Shared Services Canada (SSC)-RCMP working relationship
- Exclusions: Direct review of SSC operations, IT systems that are owned by divisions, and non-enterprise IT systems



Overall, the audit found that since the 2010 Report of the Auditor General of Canada – Chapter 1: Aging IT Systems that identified the need for the RCMP to develop an action plan and appropriate funding strategy for each significant aging IT risk, the RCMP's **progress on modernizing aging IT systems has been weak**. Specifically, we found that:

- A governance process is in place at the IM/IT Program level, including an integrated planning process to prioritize IT projects and maintenance activities. However, there are opportunities to improve organizational IM/IT governance to ensure the integrated management of aging IT systems and strategic decision making.
- [REDACTED]
- The RCMP has put in place a Digital Policing Strategy and a Digital Serge approach that aim to ensure the organization has modern digital tools and enable a dynamic policing response. However, these initiatives are focused on long-term outcomes (i.e. 5-10 years outlook), [REDACTED].

The life cycle of IT systems can be as short as 2 to 3 years before they need to be replaced. [REDACTED]

The IM/IT Program accepts the findings and recommendations of the audit. The audit has identified key areas requiring attention, which will enable the RCMP to make targeted improvements to enhance governance and make important, informed decisions in the prioritization and management of technical debt. Ultimately, implementing the recommendations will ensure better provision of modern tools and services, in support of policing operations, and enhance the department's overall effectiveness.

The achievement of the key objectives and planned actions outlined in the Management Action Plan (MAP) will be contingent upon the receipt of resources to address the recommendations, along with clear direction to align with business line priorities. Without additional resources, the IM/IT Program will not have the capacity necessary to fully implement the MAP.

Bryan Larkin

Deputy Commissioner Specialized Policing Services

2 Audit Approach

Audit Objective

The objective of this audit is to assess the adequacy and effectiveness of the RCMP’s management and modernization of its aging IT systems.

Audit Scope

The scope of the audit focused on the inventory of enterprise-wide, aging IT systems between fiscal years 2018-2019 and 2022-2023; the RCMP’s IT investment plans, governance structures; and key modernization projects in place to address the inventory of aging IT systems, including key data indicators used to report on progress.

Detailed audit testing was conducted on a sample of four aging IT systems to assess the risks and challenges of these aging systems and impacts to the organization:

- Criminal Justice Information Management (CJIM)
- Computerized Integrated Information and Dispatch System (CIIDS)
- Oracle Database
- Microsoft Windows Servers

The scope excluded a direct review of SSC operations to manage and modernize IT systems that are not owned by the RCMP. However, the audit considered the working relationship between the RCMP and SSC, and the impacts of SSC operations to the organization. The scope also excluded detailed audit testing on IT systems that are owned by divisions*, and non-enterprise IT systems (e.g. managed by Technical Operations).

KEY THEMES

The audit findings are grouped into the following 3 key risk areas for the organization:

1	IM/IT Governance
2	Management of IT Systems
3	Management of Technical Debt


* Although divisional systems were excluded from the scope of this audit, the audit team noted during the planning phase of this engagement that divisional systems were a significant risk area for the IM/IT Program in that there is a lack of visibility over divisional systems that may lead to duplication of effort, incompleteness of data, and increased cybersecurity risks and costs. This risk area will be considered as part of internal audit’s risk-based audit planning process.

The audit was conducted between July 2023 and June 2024. The audit team employed various audit techniques including:

Interviews with RCMP Employees

In-person and video interviews were conducted with individuals in a variety of areas within the RCMP:


- IM/IT Program
- Divisional Informatics Officers
- Departmental Security
- Contract and Indigenous Policing and Specialized Policing Services (i.e. business owners)
- Financial Management Advisors
- Policy Centres – Equity, Diversity, and Inclusion (EDI)/ Gender-based Analysis Plus (GBA Plus), Accessibility, Official Languages



Document Review

Documents were reviewed from a variety of sources:


- Treasury Board (TB) policies, directives and guidelines; and RCMP manuals
- Committee terms of references and records of decisions
- RCMP’s Departmental Plan on Service and Digital and Integrated Plan; investment plans and strategic plans
- Best practices – e.g. Office of the Chief Information Officer (OCIO) guidelines, Control Objectives for Information and related Technology (COBIT), Gartner, ISACA, other government departments
- SSC/RCMP business arrangement and related work
- Previous Internal Audit, Evaluation and Review (IAER) reports



Audit Testing and Data Analysis

To assess the risks and impacts of aging IT systems, the following testing approach was conducted:

- Analysis of application portfolio management
- Analysis of IT maintenance plans
- Analysis of IT system prioritization
- Analysis of IT inventory
- Analysis of IM/IT resourcing structure
- Analysis of IM/IT management of software versions



Case Studies

A sample of four aging IT systems was selected to analyze system incidents using the RCMP’s Service Desk Manager (SDM) data:

- **CJIM** – an application created to facilitate the automating and streamlining of the criminal record information. Used by the RCMP and Canadian law enforcement partner agencies.
- **CIIDS** – an application that serves the Computer Aided Dispatch and RCMP Operational Communication Centres that handle 9-1-1 calls and dispatch RCMP members.
- **Oracle Database** – provides a common option for database management services and consistent control of data.
- **Microsoft Windows Servers** – an operating system that supports applications, data storage and network communication.

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’s Directive on Internal Audit, as supported by the results of the quality assurance and improvement program.



3 Organizational Context

- A. Timeline of Key Events
- B. RCMP Risk Drivers
- C. What are Aging IT Systems?
- D. Roles and Responsibilities
- E. RCMP-SSC Business Arrangement

Report of the Auditor General of Canada – Chapter 1: Aging IT Systems
Recommended that the RCMP develop an action plan for each significant aging IT risk, and identify an appropriate funding strategy for its aging IT systems.

Treasury Board Secretariat (TBS) – Report on the State of Aging IT Across the Government of Canada
Determined that application portfolio management is not consistently practiced across government departments; thereby supporting the need for a formalized approach to manage applications.

Launch of Application Portfolio Management (APM) Program
TBS introduced the APM program in response to the 2010 Report of the Auditor General of Canada – Chapter 1: Aging IT Systems.

RCMP’s Corporate Risk Profile
Sustainability of aging IM/IT systems and overloaded data holdings pose significant risks to meeting administrative and operational requirements.

RCMP’s ongoing response to Auditor General of Canada’s report
RCMP advanced the implementation of an enterprise approach to IM/IT; developed maintenance plans to integrate evergreening of aging IT systems; and implemented TBS’ APM program. However, challenges continued in ensuring adequate funding.

Vision 150 & Digital Policing Strategy
Established to ensure the RCMP has the right capabilities to deal with the digital era’s impact on policing.

SSC’s Workload Migration Program
Objective was to facilitate the migration of government applications and data from aging, legacy data centres to modern, more secure and reliable solutions.

Mass Casualty Commission (MCC) Report
Highlighted issues with aging IT systems and infrastructure, lack of integrated or incompatible systems with external partners, and inability to bring on new technology on outdated systems and aging software.
Note: The MCC stated there was no evidence to suggest aging IT contributed to shortcomings identified in the report.

IAER’s Targeted IM/IT and Information Security Planning Study
Identified aging IT systems as a high-risk area. Current controls, organizational mechanisms, and organizational approach to risk identification, prioritization and mitigation for IT systems are not sufficient to address the current state of aging IT systems at the RCMP.

Report 7 of the Auditor General of Canada – Modernizing IT Systems
Identified that the funding approach for federal departments to address immediate and future costs of modernization is inflexible; leaving limited mechanisms for departments to obtain sufficient funding to meet their modernization needs.





IAER's 2023 Targeted IM/IT and Information Security Planning Study identified various organization-wide risk drivers impacting the current state of aging IT systems:

Decentralization and Governance

- Evolving governance structure - the composition of national committees has been in flux over the last few years, in addition to notable senior executive turnover.

Planning and Prioritization

- Since 2021, the RCMP's strategic planning process has been in an evolving state of development.
- Operational requirements supersede enabling function needs, often resulting in priorities shifting because of current events.

Funding

- Disconnect between the strategic planning process and the annual budgeting process.
- As per the 2024-28 RCMP Investment Plan, 63% of the IM/IT Program's budget sustains activities associated with existing services; only 16% is spent on transformation.

Resourcing and Capacity

- There is difficulty attracting skilled resources due a competitive job market. There is an increased reliance on external/contract expertise to fill gaps in skills and resources. There is a need to focus on employee retention.

Transformation and Modernization

- Several initiatives are underway across the RCMP, however, there is limited integration between initiatives and alignment to strategic objectives.

Corporate Culture

- The RCMP's risk appetite and corporate culture (i.e. reactive rather than proactive) impacts the modernization of aging IT systems, in that IT systems are often addressed when they are broken/in a critical state.

SSC

- SSC and the RCMP have faced challenges, including coordinating IT infrastructure activities, and adhering to security requirements and contract policing obligations, which impact the RCMP's IM/IT planning.

Aging IT Systems

Technology (i.e. applications and infrastructure) that may be meeting current business needs, but is aging and not evolving thus becoming increasingly expensive to operate and may pose certain risks such as cybersecurity risks, and operating risks (i.e. risk of system failure).

Legacy IT Systems

Technology that is outdated or obsolete, and as such, is no longer supported, incompatible with newer technology, and requires support from specialists with a niche skillset.

Technical Debt

The accumulation of future costs such as maintenance, as a result of not keeping existing IT systems up to date or investing in new technology. As technical debt grows, there is a risk of higher costs when those actions can no longer be avoided (i.e. end-of-life), and service delivery and cybersecurity become riskier.



IM/IT Program (core units involved in the management of aging IT)

Chief Information Officer (CIO)

- Manage departmental IT
- Advise on digital enablement to meet government priorities and business needs
- Ensure IT management practices align with TBS-OCIO direction, and legislation and policies

Digital Systems and Solution Delivery (DSSD)

- Application development
- Implementation and maintenance of operational and administrative systems

Operations and Platform Support (OPS)

- IT support services (e.g. common services)
- Help Desk
- Infrastructure maintenance
- Application testing

Digital Strategy, Governance and Program Support (DSGPS)

- Strategic guidance
- Project delivery office
- SSC-RCMP client relationship
- Intake of client requests

SSC

- Deliver and support enterprise-wide IT infrastructure to federal departments and agencies

Departmental Security (core units involved in the management of aging IT)

Information and Communications Technology Security

- Promote risk mitigation measures to safeguard IT systems
- Align to GC policy requirements
- Security risk assessments and authorization
- Verify security compliance
- IT security advice and guidance

Chief Transformation Officer (CTO)

- Advance digital transformation
- Change management
- Cultivate digital fluency

Business Owners

- Identify business priorities and communicate them to the IM/IT Program
- Funding IT projects

Divisions

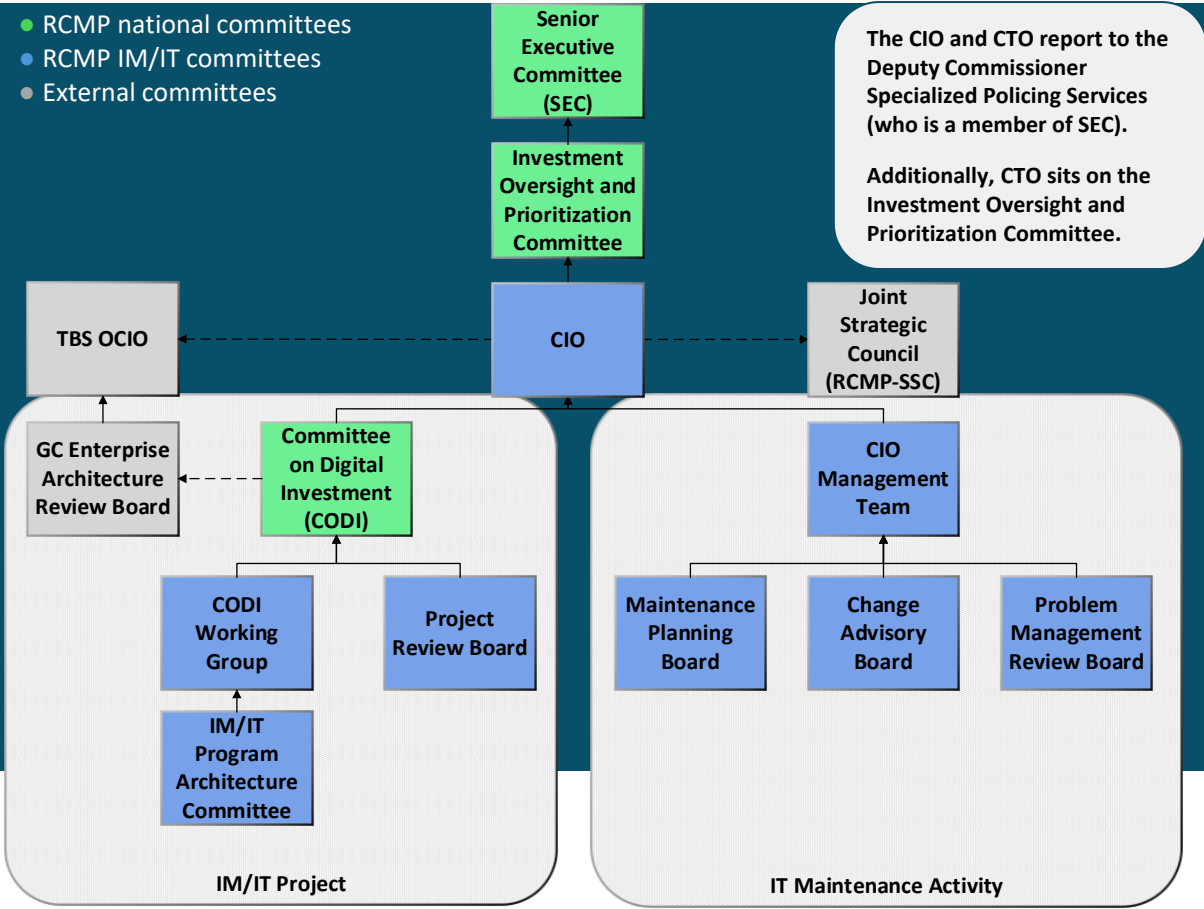
Commanding Officers

- Manage divisional IT
- Manage divisional IT funding

Divisional Informatics Officer

- Divisional IM/IT services
- Ensure alignment to national standards

Figure 1: IM/IT Governance Structure



- SSC provides enterprise-wide digital services to 45 federal department and agencies, enabling departments and agencies to deliver digital programs and services that meet the needs of Canadians.
- Recognizing the sensitive and mission-critical nature of RCMP operations, SSC established a dedicated group known as **SSC Policing Infrastructure Operations (PIO)** to specifically support the RCMP's unique operational requirements.
- A business arrangement between the RCMP and SSC outlines the roles and responsibilities of both organizations, with an SSC Director General holding full operational accountability for delivering SSC services to the RCMP. This **dedicated team includes personnel exclusively focused on supporting the RCMP, with an increased emphasis on divisional support**. Their responsibilities encompass account management, service management, data center services, email, and most network services.
- There are **significant dependencies with SSC** owned components, as such, SSC has been part of RCMP's IM/IT governance committees and working groups responsible for developing RCMP IT maintenance plans and resolving RCMP IT incidents to improve alignment. However, despite close collaboration between SSC and RCMP, **SSC maintenance activities (and aging infrastructure) may impact the RCMP's systems**, which can cause issues such as outages and degradation of services.



The scope of SSC's and RCMP's responsibilities as outlined in the Business Arrangement:

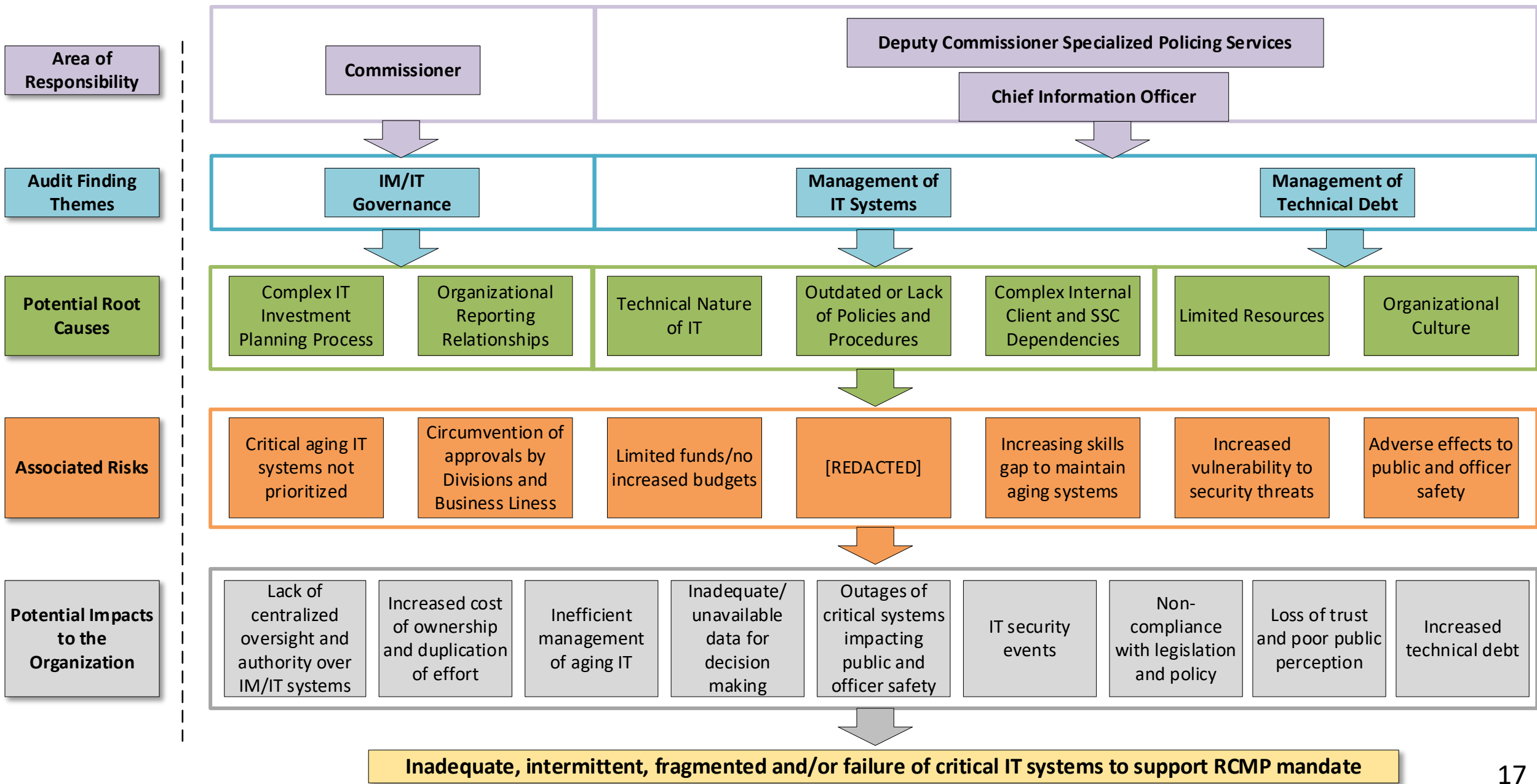
SSC	RCMP
<ul style="list-style-type: none">• Email systems• National networks• Data centres• IT infrastructure• IT security (over IT infrastructure)• Telephony (wired and cellular)	<ul style="list-style-type: none">• Business applications• Radios and mobile workstations• Technical (policing) operations• Forensic Science and Identification Services Labs• Top Secret (Classified Environment) systems

4 Key Audit Findings

- A. Summary of Issues and Impacts
- B. IM/IT Governance
- C. Management of IT Systems
- D. Management of Technical Debt

Summary of Issues and Impacts

Unclassified

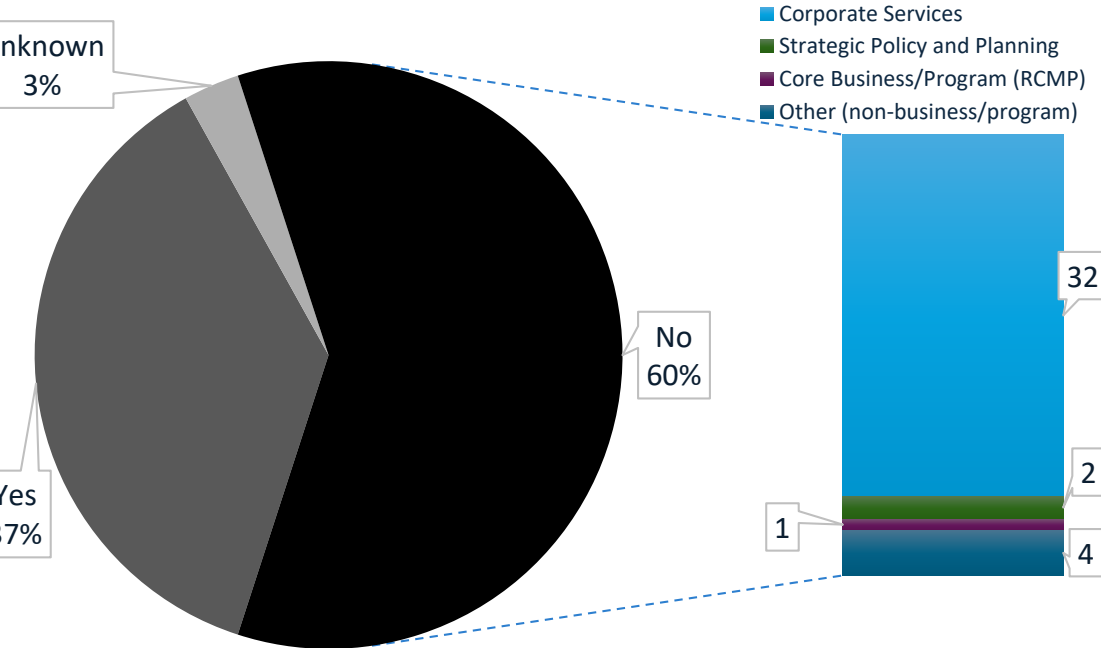


Finding 1: There are opportunities to improve organizational IM/IT governance to ensure the integrated management of aging IT systems and strategic decision making.

Table 1: Proportion of Items Discussed at National Committees that are related to Aging IT (2018-23)

National Committee		
Tier I	Senior Executive Committee	14%
	Senior Management Team	25%
Tier II	Management Committee	19%
	Policy Committee	16%
	Investment Oversight and Prioritization Committee	21%
	National Integrated Operations Committee	0%

Figure 2: Benchmark of Other Government Departments' CIOs Reporting Directly to a Deputy Head



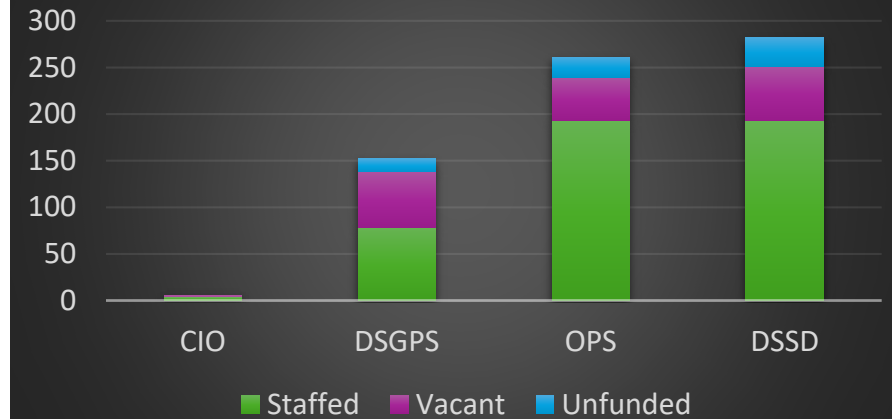
Key Observations

- The audit found that a governance process is in place at the IM/IT Program level with linkage to the RCMP's national committee governance structure, however, there is a **lack of documented processes and updated policies** (e.g. Informatics Manual, part 3 – Information Technology Standards was last updated in 2007), which can lead to misunderstanding of roles and responsibilities of key stakeholders. (See Figure 1, Slide 10)
- The IM/IT Program has an integrated planning process in place to prioritize IT projects and maintenance activities, however, the audit found **gaps in how aging IT risks are addressed and/or understood by Business Owners and national tiered committees**. For example, the decision to address an aging IT risk (e.g. end-of-life, end of vendor support) often rests with the Business Owner who may prioritize new enhancements rather than addressing aging IT risks - "just an IT upgrade." As per Table 1, at the national committee level, **aging IT risks are not prominently reflected and may lose relative position** when competing with other Government and policing priorities.
- The TB Policy on Service and Digital requires that the departmental CIO have direct access to the deputy head (i.e. Commissioner). Supporting policy guidelines suggest that depending on the department's organizational structure, direct access can be achieved by:
 - Reporting directly to the deputy head
 - Having regular bilateral meetings with the deputy head
 - Being a member of the executive committee
 - Communicating directly with the deputy head as needed
- The RCMP's IM/IT Program is under the functional leadership of the CIO, who reports administratively to the Deputy Commissioner of Specialized Policing Services (one of three core RCMP mandates). The CIO has identified that there is a direct line of communication to the Commissioner if and when needed. In addition, the CIO is a member of the Senior Management Team committee (chaired by the Commissioner) that is responsible for providing advice and recommendations to the SEC (highest senior decision-making body at the RCMP, responsible for setting overall strategic direction and vision, also chaired by the Commissioner). The CIO does not have a permanent seat at SEC.
- As per Figure 2, benchmarking of other government departments reveals that the CIO reports: directly to the deputy head (37% of Departments), or reports to the program head of a non-core business line (58% of Departments).

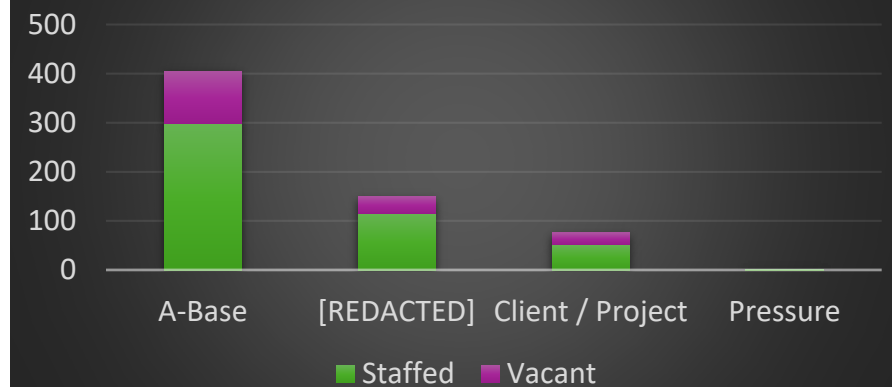
Key Observations

- Based on the IM/IT Program's internal organizational charts, the audit found that the **core units (i.e. DSSD, OPS, DSGPS and CIO)** involved in the management of aging IT had a **vacancy rate of 33%** as of December 2023 (Graph 1). Out of 33% vacant positions, 10% were unfunded positions and 23% were funded positions.
 - The audit found there were **various sources of resource funding** (i.e. A-base, [REDACTED], client/project) **with A-base funded resources accounting for 58% of the core units' resources** (Graph 2). Additionally, the CIO does not have functional authority over all IT resources (financial and personnel). This can create an **imbalance of resources specifically for IT management** – i.e. if the business owner has the funds they can fund IT positions to support their applications (e.g. HRMIS, TEAM).
 - Of note, the audit found that within DSGPS, Innovation and Architecture (unit responsible for APM in addition to enterprise architecture) represents only 3% of the core units' resources, which is a **relatively small team for the level of effort needed to manage the APM program**.
- Increasing demand for IM/IT services requires significant investment to maintain and enhance existing aging IT systems. The audit found gaps that may be impacting the effectiveness of IT investment planning:
 - Funding is decentralized in that the **CIO manages approximately 40% of the IM/IT budget, with the remainder being managed directly by divisions and business lines**. As a result, the **CIO has limited visibility and authority over the use of the majority of IT funds**, which results in a dependency on business owners (who may not have the technical expertise, or holistic perspective) to prioritize funding major IT maintenance work and/or projects addressing aging IT risks.
 - There is a **lack of long-term financial forecasting and consideration of IT maintenance costs** once a project has been implemented. This often results in the IM/IT Program absorbing maintenance costs, or if additional funding is needed, the maintenance item/project may be backlogged while competing with other national priorities. Interviewees noted that **complexities and data quality with the current RCMP financial system** may be a contributing factor to the ineffective financial forecasting across the organization (this condition is not specific to the IM/IT Program), and could be addressed when the new financial system is implemented.
 - Lastly, interviews with IM/IT Program senior officials indicated two additional **areas that affect the IM/IT Program's financial forecasting**: (1) often SSC does not recover costs by end of fiscal year, which has resulted in the IM/IT Program lapsing funds that could have been used internally to fund IT projects and/or maintenance activities, and (2) short lead-times have resulted in the IM/IT Program incurring additional costs (e.g. vendor support) because work on the RCMP side could not be completed on time.

Graph 1: IT Resources per Unit (December 2023)



Graph 2: IT Resources per Funding Source (December 2023)



Why it matters?

Improves Business Planning

- Aligns IT goals with organizational goals
- Manages the relationship between business owners and the IM/IT Program
- Improves demand and service capabilities

Defines Accountabilities

- Ensures responsibilities are known by the various groups responsible for IT prioritization
- Increases the value and stakeholders' understanding of IT investments in relation to Government and operational priorities
- Provides consistency, processes and standards to improve the effectiveness of IT operations

Reinforces Risk Management

- Drives IT risk appetite
- Improves IT risks management decisions
- Focuses operational, security and privacy requirements with IT investments

Supports IT Management

- Improves life cycle management of IT systems
- Assists the organization to adapt to the changing IT environment

Recommendation 1

The Deputy Commissioner Specialized Policing Services should:

- A. Strengthen the existing IM/IT governance process to align aging IT risks to organizational priorities, and improve the management of financial, public safety and policing risks associated with aging IT.
- B. Strengthen accountabilities of the IM/IT Program and Business Owners by reviewing and updating existing internal policies and procedures to ensure all stakeholders are aware of their areas of responsibilities, and improve reporting relationships.
- C. Strengthen IM/IT financial planning by reviewing existing financial management and data collection processes to ensure the total cost of ownership over the life of an IT system is adequately captured and presented when making IT investment decisions, and budget allocations.



Finding 2: There are opportunities to improve the management of IT systems within the RCMP to oversee its portfolio of applications, inform investment decisions, plan maintenance/decommissioning activities, and improve the RCMP's security posture.



Key Observations

- The audit found that the organization gathers APM data only once a year to report to TBS. The organization is **not actively using APM** data to manage its portfolio, nor to make investment decisions or plan the maintenance or decommissioning of applications.
- APM governance, processes, roles and responsibilities have not been defined and integrated into core IT processes, which has resulted in **inefficient and ineffective use of the APM Program**.
- Organization-wide **standards for APM** categories (e.g. business value and technical condition) **have not been defined**, which may result in risk scores not aligning to operational priorities and impact decision making.
- Visibility over the health of applications across the RCMP is **limited to enterprise-wide applications** – i.e. divisional and specialized unit applications are not captured in the APM.
- APM Program is operating in a silo, which has **limited data sharing to relevant stakeholders** (e.g. IT maintenance planning) and for internal strategic and investment decision making.
- Collection and analysis of APM data results in significant workload for the APM team (within Innovation and Architecture). Currently, there are [REDACTED] business owners are required to complete and the APM team consolidates on a yearly basis. Additionally, the **APM process is heavily dependent on manual data inputs**.
- Inefficiencies with the APM process have resulted in **poor data quality** (i.e. outdated, incomplete, unvalidated, incorrect).

[REDACTED]

[REDACTED]

[REDACTED]

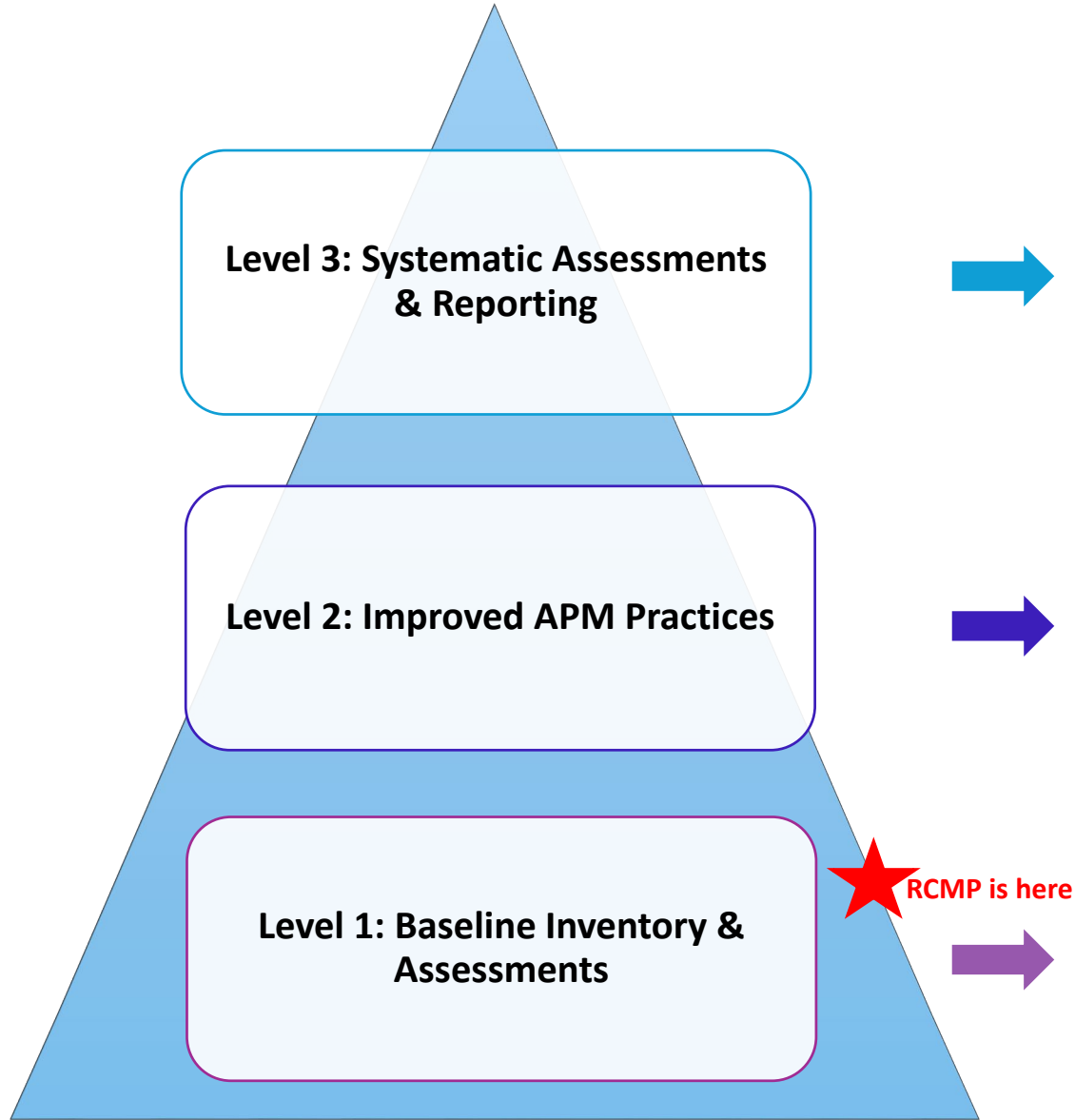
[REDACTED]

- APM’s **aging IT assessment** identifies if an application is at risk of failure due to poor technical conditions, inadequate funding and disaster recovery planning. It also indicates the urgency of action to address the application’s at-risk state.
- As per TBS, departments are expected to **monitor and communicate on a regular basis to their senior management the action plans for mission critical systems at risk.**
- [REDACTED]

- APM’s **Tolerate Innovate Migrate Eliminate (TIME) assessment** (adapted from Gartner’s TIME model) enables departments to assess their application portfolio from a business, IT and cost perspective, and aids analysis and discussion in order to identify and prioritize opportunities for improvement (Graph 4).
 - **Tolerate** — application is in good technical shape but lacking business support, so IT should tolerate the application until the business owner wants to invest in improving the application’s business fitness.
 - **Innovate** — application is in good shape, so IT should invest in it when asked to add features or turn on some new functionality of a packaged application, while also keeping it technically healthy.
 - **Migrate (or Modernize)** — application does just what the business wants, but IT is concerned with the age and brittleness of the underlying technology. If the business wants functional improvements, IT should do this by simultaneously migrating the underlying technology to current, supported technology.
 - **Eliminate (or Replace)** — these applications may be in such bad shape it is not worth spending on them. If they are not needed, or the functionality is now available in a better application, they should be eliminated. If the functionality is still needed, they might need to be replaced.

APM Program Maturity Model

(Source: TBS-OCIO APM User Guide)



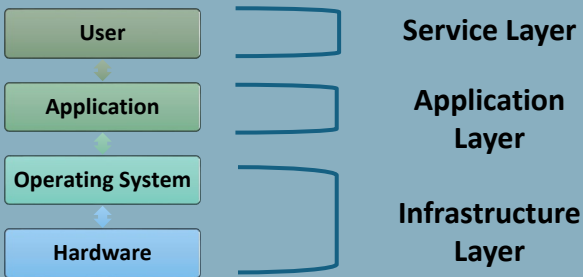
- APM governance, processes, roles and responsibilities are applied
- Plans and funding are in place to proactively manage the life cycle of each application
- APM team actively reviews and approves “Business Value” and “Technical Condition” ratings based on organizational rating standards
- Investment decisions are made based on the analysis of the APM and integrated with the IT Investment Plan
- APM processes are continuous, systematic and improve over time
- APM is used to measure performance and effectively used to control the portfolio

- APM governance, processes, roles and responsibilities of stakeholders are defined
- Application business owners are involved in the assessment of their applications
- Organization-wide standards for “Business Value” and “Technical Condition” are developed
- Strategic planning and investment decisions take into account APM data
- Product roadmaps are developed to rationalize the portfolio, reduce number of applications with redundant functionality, and achieve cost savings
- Regular oversight and reporting to senior management are in place

- Application inventory exists
- Mission-critical applications are identified
- Applications at risk of aging are identified
- Investment decisions regarding application sustainability and retirement are reported in the IT Investment Plan

IT Maintenance Planning

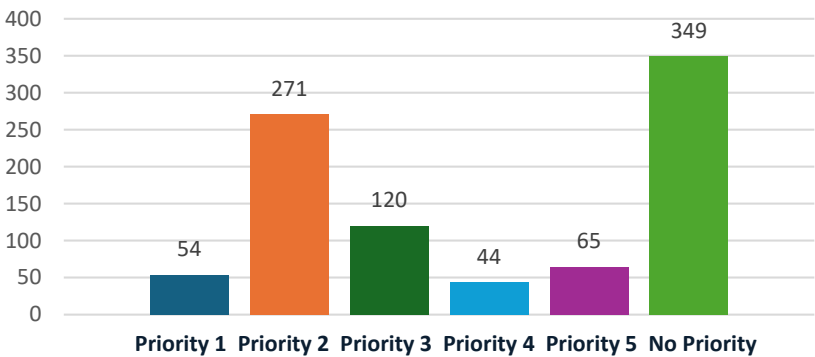
- Maintenance planning defines mandatory work needed to keep business applications and IM/IT services running effectively, while considering new developments. Maintenance impacts the service, application, and infrastructure layers. If systems are not regularly maintained or effectively monitored, it exposes them to cybersecurity risks. At the RCMP, there have been instances where servers running obsolete operating systems have been found with vulnerabilities for which security patches do not exist (i.e. zero-day vulnerabilities).
- Annually, IT Service Management collects the infrastructure maintenance activities and milestones, and coordinates with the application side to develop the annual IT Maintenance Plan. IT maintenance work is categorized into five priority levels.
 - Priority 1** – mandated, Government, or legislative requirements
 - Priority 2** – end-of-life, end of support, security vulnerabilities and/or older version of software
 - Priority 3** – major bug fixes, health issues, and/or older version of software
 - Priority 4** – minor bug fixes or minor enhancements
 - Priority 5** – none of the above



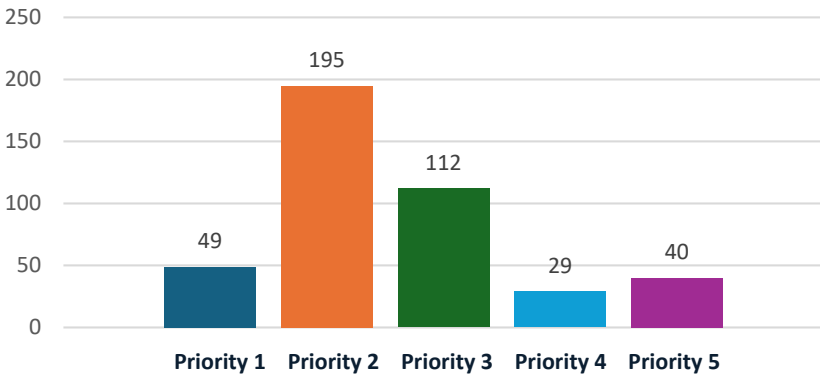
Key Observations

- Although IM/IT senior management has **mandated work on priority 1 and 2 activities** (the latter addresses aging IT risks), the scheduling of these activities is **dependent on the availability of funding and resources**. Interviewees noted that other priorities (i.e. 3 to 5) can take precedence because of various factors such as:
 - Client pressures – e.g. the client is funding IT resources, or
 - The IM/IT Program cannot work on a priority 1 or 2 because of delays – e.g. dependency on SSC to complete their component before the RCMP can continue maintenance work

Graph 5: Forecasted Maintenance Items by Priority Level (2018-23)



Graph 6: Completed Maintenance Items by Priority Level (2018-23)



- As per Graph 5 and 6, the audit team conducted an analysis of the IT Maintenance Plans to assess the population of forecasted maintenance work versus actual work between fiscal years 2018-19 and 2022-23:
 - Of the 903 maintenance items assessed **425 (47%) of the forecasted maintenance items were noted as complete.**

Key Observations

- Presently, the IM/IT Program has a manual IT maintenance process in place; [REDACTED].
- [REDACTED]
- [REDACTED]



Table 2: Analysis of Infrastructure Versions

Oracle Database Versions (as of January 2024)			Windows Server Versions (as of March 2024)		
Oracle Version	Total Databases per Version	The standard version for this infrastructure component is Oracle [REDACTED]; however, there are still Oracle databases running on [REDACTED] due to delays with meeting application requirements.	Windows Version	Total Servers per Version	The RCMP is running [REDACTED]. The [REDACTED] except for [REDACTED] as part of SSC’s Windows Modernization Program.
[REDACTED]	[REDACTED]		[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]		[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]		[REDACTED]	[REDACTED]	
Total Oracle Databases	[REDACTED]		Total Windows Servers	[REDACTED]	

- Audit testing (Table 2) found that when an upgrade is available, the infrastructure group will advise application owners so they can provide their milestones to meet infrastructure changes.
- However, interviewees noted **meeting infrastructure timelines are for the most part dependent on application requirements, resources and level of prioritization.**

- For non-RCMP owned infrastructure, the audit found that the IM/IT Program does not have access to **SSC’s infrastructure maintenance schedule, which often has affected the IM/IT Program meeting SSC deadlines and has impacted RCMP applications (e.g. application glitches, outages) when SSC carries out infrastructure upgrades on the underlying network with short lead-times.**
- This gap has been identified by RCMP stakeholders and communicated to SSC through various joint governance committees. However, **the information needed to work collaboratively and integrate RCMP maintenance activities with those of SSC is not readily available.**

Why it matters?

Improves Business Value

- Prioritizes system investments
- Assesses business value of systems and decommissions those with low business value
- Provides an enterprise view to support alignment with departmental priorities

Minimizes Risks

- Aligns system portfolio to policies and guidelines
- Identifies systems at risk due to aging IT
- Prioritizes critical business applications and systems
- Ensures reliable, available, secure systems with minimal downtime and maximizing productivity

Supports Modernization

- Identifies the need for upgrades for systems reaching end-of-life
- Assesses compatibility of applications when modernizing the infrastructure layer
- Assists with developing application roadmaps with business owners

Increases Enterprise Oversight

- Provides a central source of data for all applications and systems
- Enables focus on systems with the highest business value for the organization

Recommendation 2

The Deputy Commissioner Specialized Policing Services should:

- A. Enhance the working relationship and communication between the IT stakeholders (i.e. application owners, infrastructure owners and business owners) to strengthen the integrated management of aging IT systems.
- B. In consideration of the IM/IT Program's existing work on revamping IT priority levels, TBS-OCIO guidelines and work performed by other government departments, improve the maturity of the APM program within the RCMP by formally defining APM governance, processes, roles and responsibilities, including all relevant stakeholders in the discussion.
- C. [REDACTED]



Finding 3: There are opportunities to improve the management of RCMP's technical debt by formally identifying, communicating and prioritizing technical debt in order to align organizational priorities, reinvest in new technology, and minimize operating costs, system failures, and vulnerabilities to cybersecurity incidents.



SSC's Workload Migration Program (WLM)

- In 2018, SSC established WLM to facilitate the migration of government applications and data from aging, legacy data centres to modern, more secure and reliable solutions – i.e. the Cloud, Enterprise Data Centre, or a hybrid of the two. WLM received funding over six years for SSC's partner departments and agencies to modernize and migrate applications from legacy data centres.
- Within the RCMP, the following projects have been approved as part of the WLM: [REDACTED].
- To effectively plan for WLM, the RCMP is required to analyze its application portfolios to determine strategies for modernizing at-risk technologies, including a plan and cost estimates. However, due to insufficient funding, migration work related to approved data centres has stalled.

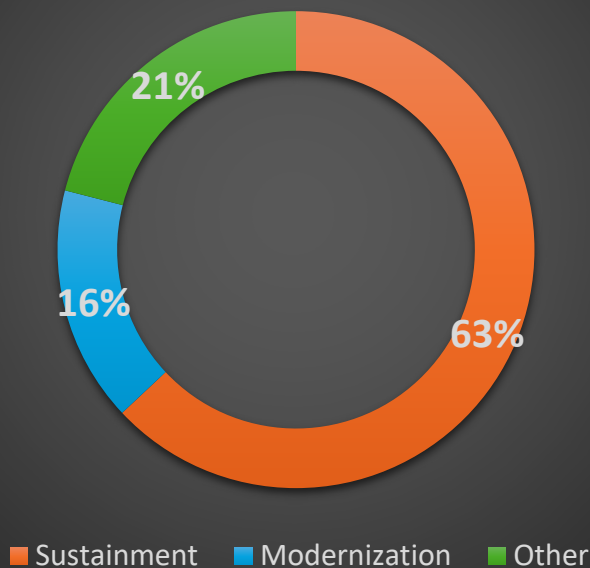
RCMP's Digital Policing Strategy

- The Digital Policing Strategy is focused on ensuring the RCMP has the right technology required to deliver and enable modern policing and public safety services.
- Three years since its launch, the RCMP is refreshing its digital objectives, assessing progress and re-focusing its future direction.
- An updated digital enterprise roadmap is currently being developed to ensure the organization is advancing the foundational technology and organizational capabilities needed to effectively respond to an ever-changing organizational digital landscape.

RCMP's Transformation Office

- In 2023, a Chief Transformation Officer position was created with the objective of advancing digital transformation to enable business transformation in support of RCMP operations.
- Led by the Transformation Office, the "Digital Serge" approach to transformation will focus on the RCMP's ability and agility to adopt advanced digital technologies.
- The Transformation Office is also working on the future architecture (i.e. Cloud) and mapping out what the RCMP will need to achieve this future state. The intended timeline is 2030, at which point, the plan would move to the IM/IT Program to implement.

Figure 3: Overview of IM/IT Program Budget Spending



Key Observations

- ▶ The audit found that the **RCMP does not have an established long-term technical debt strategy** to evaluate and prioritize the highest risk items, and create awareness and buy-in from senior management. The following organizational barriers may be impeding the development of an effective RCMP-wide technical debt strategy:
 - [REDACTED]
 - Systematic lack of funding across business lines, which [REDACTED]. Based on the 2024-28 RCMP Investment Plan (see Figure 3), only 16% of the IM/IT Program's budget is spent on modernization.

- IT projects face **delays at various stages, which sets back realized benefits of new technology**. For example, often projects remain on the backlog list (i.e. unfunded projects) for years until sources of funds become available. Once a project is approved, it may face additional delays at the procurement stage depending on the monetary value and the complexities of procurement.
- In some instances, there may be legal holds on information including information collected through RCMP IT systems. As such, **information retention may become a barrier to eliminate obsolete IT systems**.
- Organizationally, **IT upgrades (i.e. maintenance) have been deferred or not prioritized in favor of other projects or priorities**. Assessing the current IT technical debt, and eliminating and/or modernizing old/underused IT allows for opportunities to reduce technical debt and reinvest funds into new technologies or sustainment activities.

In the absence of a technical debt strategy, the RCMP continues to address existing aging IT systems while balancing competing priorities. For example, the RCMP recently approved an investment for the Computer Aided Dispatch Next Generation project, which is expected to replace the 25+ year CIIDS system [REDACTED]. Although the CJIM Rewrite is an unfunded project, the IM/IT Program recently authorized an options analysis to help build a business case moving forward. Additionally, in 2023, the RCMP decommissioned three legacy systems – two were migrated to new modern systems, and one was no longer in use; 11 servers were decommissioned as a result of these decommissioned systems and/or infrastructure evergreening.

- The audit found that the IM/IT Program **may not actively consider policy requirements** (such as accessibility, EDI, official languages, and GBA Plus) **when replacing or updating its aging IT systems**. Currently, the IM/IT Program does not oversee the assessment of these requirements across IM/IT projects; therefore, it is **not clear whether these steps are concretely considered when planning for the replacement of IT systems**.
- Policy centres (i.e. GBA Plus, EDI, accessibility and official languages) expressed that presently they are not resourced to conduct a full analysis for each system; therefore, their role is to advise and consult on request. Of the four IT systems sampled, interviewees **did not indicate any known instances of non-compliance** with official languages, accessibility, EDI and/or GBA Plus.
- Applying policy requirements can help ensure the needs of diverse groups of people are embedded in the decision-making process at all stages of an IT project. In addition, implementing these requirements afterwards can be more difficult and costlier.



Why it matters?

Planning for the Future

- Legacy systems supported by old infrastructure are at risk of breaking down, potentially preventing the RCMP from delivering services to the public.
- Long-term planning and budgeting is needed to align national and divisional priorities and support modernization, which can take years to implement – i.e. the cost of decommissioned systems can be reinvested into new technologies.

Support Funding Requests needed to reduce Technical Debt

- TBS' Technical Debt Working Group has stopped for budgetary reasons.
- This was a potential funding source that the RCMP will be unable to draw from to reduce its technical debt, so the RCMP will need to find another way to fund these needs.

Short Life Cycle causes Technical Debt to grow

- The life cycle of new technology is getting shorter, and falling behind will increase the RCMP's cybersecurity risk.
- The vendor provides limited to no support for end-of-life technology. This increases maintenance costs significantly. Aging IT systems have limited capacity to integrate with other IT systems.

Recommendation 3

The Deputy Commissioner Specialized Policing Services should:

- A. In consultation with Tier 1 and Tier 2 RCMP governance committees, as appropriate, develop an action plan that will proactively address technical debt within the RCMP and help manage the future accumulation of technical debt. As part of the action plan, consultation should occur with all relevant stakeholders including policy centres such as Official Languages, Accessibility, GBA Plus and EDI to ensure adherence to these policy requirements in planning of new and replacement systems moving forward.



5 Case Studies

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

6 Conclusion

A. Key Takeaways

B. Recommendations

- Overall, the audit found that since the 2010 Report of the Auditor General of Canada – Chapter 1: Aging IT Systems that identified the need for the RCMP to develop an action plan and appropriate funding strategy for each significant aging IT risk, the RCMP's progress on modernizing aging IT systems has been weak. Specifically, the audit found that:
 - A governance process is in place at the IM/IT Program level, including an integrated planning process to prioritize IT projects and maintenance activities. However, there are opportunities to improve organizational IM/IT governance to ensure the integrated management of aging IT systems and strategic decision making.
 - [REDACTED]
 - The RCMP has put in place a Digital Policing Strategy and a Digital Serge approach that aim to ensure the organization has modern digital tools and enable a dynamic policing response. However, these initiatives are focused on long-term outcomes (i.e. 5-10 years outlook), [REDACTED].
- The life cycle of IT systems can be as short as 2 to 3 years before they need to be replaced. [REDACTED]



The Deputy Commissioner Specialized Policing Services should:

IM/IT Governance

1

- A. Strengthen the existing IM/IT governance process to align aging IT risks to organizational priorities, and improve the management of financial, public safety and policing risks associated with aging IT.
- B. Strengthen accountabilities of the IM/IT Program and Business Owners by reviewing and updating existing internal policies and procedures to ensure all stakeholders are aware of their areas of responsibilities, and improve reporting relationships.
- C. Strengthen IM/IT financial planning by reviewing existing financial management and data collection processes to ensure the total cost of ownership over the life of an IT system is adequately captured and presented when making IT investment decisions, and budget allocations.

Management of IT Systems

2

- A. Enhance the working relationship and communication between the IT stakeholders (i.e. application owners, infrastructure owners and business owners) to strengthen the integrated management of aging IT systems.
- B. In consideration of the IM/IT Program’s existing work on revamping IT priority levels, TBS-OCIO guidelines and work performed by other government departments, improve the maturity of the APM program within the RCMP by formally defining APM governance, processes, roles and responsibilities, including all relevant stakeholders in the discussion.
- C. [REDACTED]

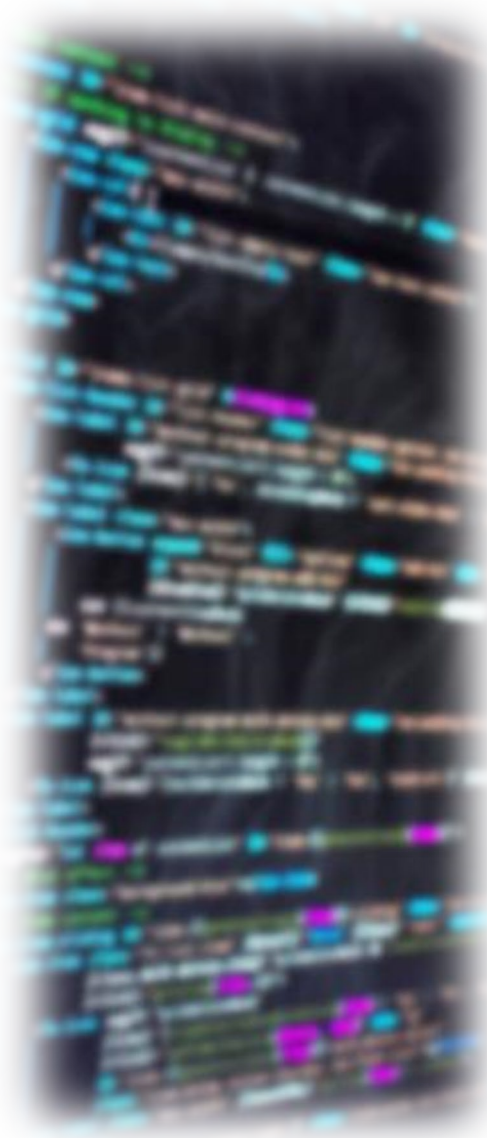
Management of Technical Debt

3

- A. In consultation with Tier 1 and Tier 2 RCMP governance committees, as appropriate, develop an action plan that will proactively address technical debt within the RCMP and help manage the future accumulation of technical debt. As part of the action plan, consultation should occur with all relevant stakeholders including policy centres such as Official Languages, Accessibility, GBA Plus and EDI to ensure adherence to these policy requirements in planning of new and replacement systems moving forward.

6 Appendices

- A. Acronyms
- B. Audit Criteria
- C. Management Action Plan



APM	Application Portfolio Management
[REDACTED]	[REDACTED]
CIO	Chief Information Officer
CIIDS	Computerized Integrated Information and Dispatch System
CJIM	Criminal Justice Information Management
CMDB	Configuration Management Database
COBIT	Control Objectives for Information and related Technology
CODI	Committee on Digital Investment
CTO	Chief Transformation Officer
DSGPS	Digital Strategy, Governance and Program Support
DSSD	Digital Systems and Solutions Delivery
EDI	Equity, Diversity, and Inclusion
GBA Plus	Gender-based Analysis Plus
HRMIS	Human Resources Management Information System
IAER	Internal Audit, Evaluation and Review
IM/IT	Information Management/Information Technology
ISACA	Information Systems Audit and Control Association
IT	Information Technology
MCC	Mass Casualty Commission
OCIO	Office of the Chief Information Officer
OPS	Operations and Platform Support
PIO	Policing Infrastructure Operations
RCMP	Royal Canadian Mounted Police
SEC	Senior Executive Committee
[REDACTED]	[REDACTED]
SSC	Shared Services Canada
TEAM	Total Expenditure Asset Management
TIME	Tolerate Innovate Migrate Eliminate
TB	Treasury Board
TBS	Treasury Board Secretariat
WLM	Workload Migration

AUDIT OBJECTIVE

To assess the adequacy and effectiveness of the RCMP’s management and modernization of its aging IT systems.

AUDIT CRITERIA

The criteria were developed primarily from Treasury Board’s policies, directives, and guidelines, as well as the COBIT framework.

Criterion 1: An effective governance structure to oversee the management of aging IT systems is in place across the RCMP.

Criterion 2: The RCMP is effectively identifying and assessing risks associated with the current state of enterprise-wide, aging IT systems to inform prioritization and funding decisions.

Criterion 3: The RCMP is effectively prioritizing and funding modernization initiatives targeting enterprise-wide, aging IT systems to reduce adverse impacts to the achievement of the RCMP’s mandate.

Audit Recommendation	Area of Responsibility	Planned Action	Diary Date
<p>1. The Deputy Commissioner Specialized Policing Services should:</p> <p>A. Strengthen the existing IM/IT governance process to align aging IT risks to organizational priorities, and improve the management of financial, public safety and policing risks associated with aging IT.</p>	<p>Many areas both in NHQ and Divisions must collaborate to gather the information required in the Application Portfolio Management (APM), both on aging systems and tools. A lot of work has already been accomplished but some gaps were identified as the data was gathered. This exercise is a great opportunity for the RCMP to deep dive and gain a deeper understanding of the current environment while heightening awareness of the RCMP's infrastructure, in a complex environment that is undergoing many transitions.</p>		
	<p>Director General, Digital Strategy, Governance & Program Support</p>	<p>Agree</p> <p>A. The IM/IT Program will review and strengthen the IM/IT governance process by:</p> <ul style="list-style-type: none">○ Conducting a thorough assessment of existing governance processes and making improvements, where possible.○ [REDACTED]○ Increasing efforts to align investments to address technical debt with business line priorities, as available funding is identified.○ Put in place a dedicated team from areas within the Program (tiger team) that will focus on increasing visibility and addressing gaps identified in the APM review in a concerted effort to maximize the reduction of organizational technical debt. <p>Interim measures:</p> <ul style="list-style-type: none">○ To begin the process, the IM/IT Program will establish a roadmap to sequence the management and prioritization of the evergreening process by June 2025.○ [REDACTED]○ Track and report on the progress of aging IT that has been replaced or decommissioned at least annually.	<p>July 2026</p>

Audit Recommendation	Area of Responsibility	Planned Action	Diary Date
<p>1. The Deputy Commissioner Specialized Policing Services should:</p> <p>B. Strengthen accountabilities of the IM/IT Program and Business Owners by reviewing and updating existing internal policies and procedures to ensure all stakeholders are aware of their areas of responsibilities, and improve reporting relationships.</p>	Director General, Digital Strategy, Governance & Program Support	<p>B. The IM/IT Program will review and strengthen IM/IT accountabilities by:</p> <ul style="list-style-type: none">Enhancing transparency and accountability by assessing and reporting on planning and evergreening efforts twice per year, beginning in May 2025.Streamlining communication channels, ensuring accessibility of evidence for informed decision-making.Reviewing and revising roles and responsibilities as well as reporting relationships.	May 2025
<p>1. The Deputy Commissioner Specialized Policing Services should:</p> <p>C. Strengthen IM/IT financial planning by reviewing existing financial management and data collection processes to ensure the total cost of ownership over the life of an IT system is adequately captured and presented when making IT investment decisions, and budget allocations.</p>	Director General, Digital Strategy, Governance & Program Support	<p>C. The IM/IT Program will review and strengthen IM/IT financial planning by:</p> <ul style="list-style-type: none">Ensuring total costs through the full lifecycle of IT systems and applications are included in the planning and costing of investments.Modernize planning/reporting systems by assessing the priority sequencing of applications and reporting on planning and evergreening efforts twice per year, beginning in June 2025.	June 2025
<p>2. The Deputy Commissioner Specialized Policing Services should:</p> <p>A. Enhance the working relationship and communication between the IT stakeholders (i.e. application owners, infrastructure owners and business owners) to strengthen the integrated management of aging IT systems.</p>	Director General, Digital Strategy, Governance & Program Support	<p>Agree</p> <p>A. To strengthen the integrated management of aging IT systems and applications, IM/IT will develop and implement, in consultation with key stakeholders, a plan for continuous improvement that will be incorporated into the periodic consultations held at least once per year with the business line leads of each system and/or application requiring modernization. This plan will be developed over the course of the next year (interim milestone: September 2025) and will be fully implemented by April 2026.</p>	April 2026

Audit Recommendation	Area of Responsibility	Planned Action	Diary Date
<p>2. The Deputy Commissioner Specialized Policing Services should:</p> <p>B. In consideration of the IM/IT Program’s existing work on revamping IT priority levels, TBS-OCIO guidelines and work performed by other government departments, improve the maturity of the APM program within the RCMP by formally defining APM governance, processes, roles and responsibilities, including all relevant stakeholders in the discussion.</p>	Director General, Digital Strategy, Governance & Program Support	<p>B. The IM/IT Program will put in place a comprehensive APM program, including the implementation of a tiger team, in consultation with relevant stakeholders, that will address the planning, prioritization and governance of an APM process that considers the costing and replacement of technology through the full life cycle of the system or application.</p> <p>Interim measures:</p> <ul style="list-style-type: none">○ 4-month (April 2025) APM data requirements and data collection methodology clearly defined for both RCMP and TBS purposes.○ 10-month (October 2025) APM data refreshed and validated and repeatable processes established.○ 12-month (December 2025) APM positions fully defined and staffed.	December 2025
<p>2. The Deputy Commissioner Specialized Policing Services should:</p> <p>C. [REDACTED]</p>	[REDACTED]	C. [REDACTED]	[REDACTED]

Audit Recommendation	Area of Responsibility	Planned Action	Diary Date
<p>3. The Deputy Commissioner Specialized Policing Services should:</p> <p>A. In consultation with Tier 1 and Tier 2 RCMP governance committees, as appropriate, develop an action plan that will proactively address technical debt within the RCMP and help manage the future accumulation of technical debt. As part of the action plan, consultation should occur with all relevant stakeholders including policy centres such as Official Languages, Accessibility, GBA Plus and EDI to ensure adherence to these policy requirements in planning of new and replacement systems moving forward.</p>	Director General, Digital Strategy, Governance & Program Support	<p>Agree</p> <p>A. The IM/IT Program will work with the Tier 1 and Tier 2 governance committee secretariats to develop an action plan that will address technical debt within the RCMP and help manage the future accumulation of technical debt. The action plan should address the prioritization of applications as funding is identified and will be done in consultation with relevant stakeholders, including policy centres such as Official Languages, Accessibility, GBA Plus and EDI to ensure adherence to policy requirements.</p> <p>Interim measures:</p> <ul style="list-style-type: none">○ Meet with all relevant business line leads to identify applications to be included on the APM and technical health defined for each application (April 2025).○ Meet with SSC to identify and schedule migration plans for applications still under RCMP responsibility (December 2025).○ Action plan for migration of all applications including sequencing will be in place (December 2026).	December 2026