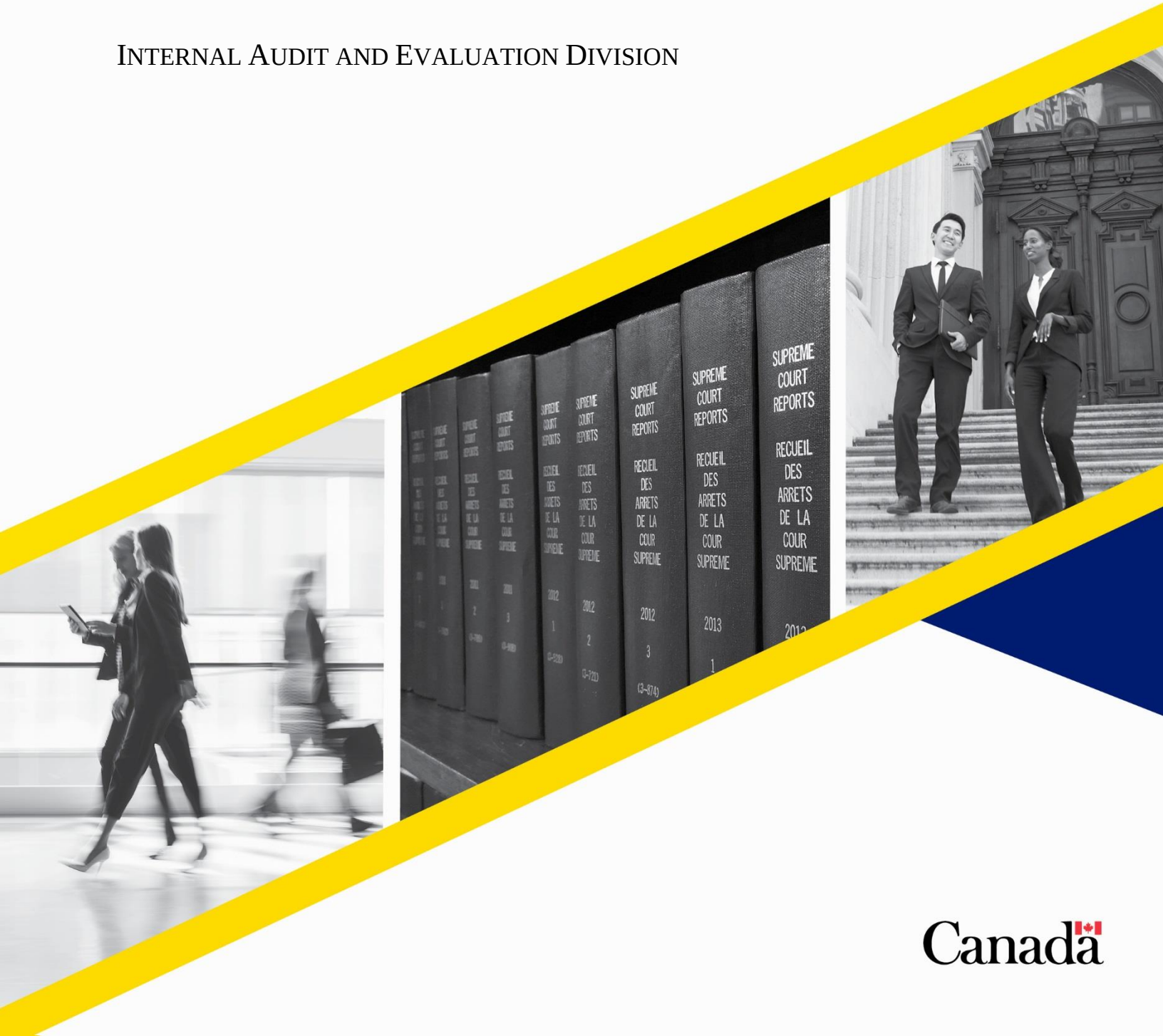
Public Prosecution Service of Canada | Service des poursuites pénales du Canada

AUDIT OF INFORMATION MANAGEMENT

FINAL AUDIT REPORT

JANUARY 2023

INTERNAL AUDIT AND EVALUATION DIVISION



Canada

As recommended by the Departmental Audit Committee, subject to approval by the Director of Public Prosecutions, on December 2, 2022.

Approved by the Director of Public Prosecutions on January 23, 2023.

Cette publication est également disponible en français.

This publication is available in HTML formats on the Internet at http://www.ppsc-sppc.gc.ca/eng/

Cat. No. J79-15/2023E-PDF
ISBN: 978-0-660-48090-9

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY

1.1 OBJECTIVES AND SCOPE

The objective of this audit was to provide management with an independent assessment of the Public Prosecution Service of Canada's (PPSC) Information Management (IM) framework to ensure that the controls are 1) appropriate, 2) are sufficient to minimize risk to the Department and, 3) are aligned with Treasury Board of Canada (TB) requirements.

The audit focused on documentation and processes relevant to the PPSC IM governance framework at headquarters and in the regions. The planning and examination phases of the audit were conducted between December 2021 and June 2022.

1.2 AUDIT CONCLUSION

The Internal Audit and Evaluation Division (IAED) assessed the adequacy and effectiveness of IM processes and frameworks against TB policies and directives. The audit found the PPSC has established fundamental elements of IM governance along with guiding IM plans and strategies. The Department follows three types of service model for IM, by which regions are either supported by local IM teams managed centrally by PPSC headquarters, by the Department of Justice (DoJ) or by local employees tasked with IM responsibilities that do not report to headquarters. We found that these three different approaches leaves IM with insufficient control and visibility in implementing plans and strategies across the organization. Additionally, expanded monitoring of IM actions and activities is needed to support oversight of IM practices and the identification of issues requiring corrective action. In the absence of monitoring PPSC's IM networks and activities, the organization may face reduced efficiencies, increased costs, non-compliance and susceptibility to security threats.

The audit also found that the PPSC has a rigorous framework of PPSC policies, directives, and guidelines in place to support effective IM. The current framework provides guidance for IM throughout its life cycle, and its policies and directives align with TB policies. Despite this guidance, measures to manage PPSC information assets are applied inconsistently. The inconsistent application of IM guidance and policies threatens the confidentiality, integrity, and availability of the PPSC's information assets.

1.3 SUMMARY OF RECOMMENDATIONS

We found that the IM directorate is committed to improving overall operations and IM awareness across the organization, including significant improvements in documenting and implementing IM policies and directives over the past three years. The PPSC has also strengthened its digital holdings through the migration of corporate and prosecution documents to the organization's central IM repository (GCdocs).

The report contains the following recommendations:

- The Director General of Administration Services Branch should:
  - strengthen oversight over information assets by implementing monitoring mechanisms to measure and provide regular reporting on activities related to information management.
  - ensure that a records disposition program is implemented to alleviate the financial impacts and minimises the amount of information maintained that no longer has business value.
  - implement a systematic approach to identify and assess subsets of PPSC documents of archival value to Canada.

1.4 STATEMENT OF ASSURANCE

In my professional judgment as the PPSC's Chief Audit and Evaluation Executive, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the conclusion provided and contained in this report. The audit findings and conclusion are based on a comparison of the conditions, as they existed at the time of the audit, against pre-established and approved audit criteria that were agreed upon with the PPSC's management. The findings and conclusion are applicable only to the entity examined. The audit was conducted in accordance with the Internal Auditing Standards for the Government of Canada.

I appreciate the cooperation and assistance provided to the audit team by PPSC staff in headquarters and regional offices.

Cathy Rodrigue
Chief Audit and Evaluation Executive

2.0 INTRODUCTION

2.1 BACKGROUND

The TB Policy on Service and Digital, implemented April 1, 2020, defines IM as "a discipline that directs and supports effective and efficient management of information in an organization, from planning and systems development to disposal and/or long-term preservation". With the PPSC's extensive reliance on large volumes of sensitive information, it was deemed important to assess the IM program and service delivery model.

Administration Services Directorate, overseen by the Director General, Administration Services Directorate and Chief Information Officer (DG, ASD and CIO), is responsible for the delivery of corporate support for IM. The IM directorate is managed primarily from headquarters in Ottawa in collaboration with regional offices and DoJ. The IM team is overseen by the Director, Information Management and Chief Data Officer.

Prior to 2019, the organization had one IM employee that was responsible to oversee this corporate function. In 2019, efforts began to create and staff the IM division in order to develop an IM program that would support the needs of the organization and the Government of Canada IM policy framework.

The PPSC unveiled its Digital Prosecution Strategy (DPS) to the Senior Advisory Board in October 2019. The DPS, in conjunction with the Department's IM-IT Investment Plan 2021-24, provide the basis for moving the PPSC from its current position to an improved IM program in two years.

The PPSC has and continues to make significant changes in the implementation of an information management program and service delivery model that includes, in most regions, the repatriation of IM services provided by the DoJ through a Memorandum of Understanding (MOU).

Table 1: IM service model by region

Approach	Region(s)
1. PPSC IM Services (headquarters)	British Columbia, Ontario, Saskatchewan, and National Capital Region
2. DoJ IM Services	Atlantic, Quebec, Alberta, and Manitoba
3. Regional IM Services	Yukon, Northwest Territories, and Nunavut

In addition to changes to the IM service delivery model, the PPSC is completing the migration of corporate documents to the organization's central IM repository (GCdocs). The Department will replace iCase, its legacy legal case management system, with its successor Amicus.

IAED conducted the Audit of IM in accordance with the PPSC's 2021-2022 and 2022-2023 Risk-based Audit Plan, approved by the Director of Public Prosecutions on May 4, 2021.

2.2 OBJECTIVES AND SCOPE

The objective of this audit was to provide management with an independent assessment of the PPSC's IM framework to ensure that the controls are 1) appropriate, 2) are sufficient to minimize risk to the Department and, 3) are aligned with TB requirements. The audit reviewed documents and processes relevant to the IM framework to provide assurance that the controls in place meet TB requirements.

2.3 METHODOLOGY

The audit work was carried out from December 2021 to June 2022. The audit methodology included the following:

- Interviews with IM management and employees;
- Review and analysis of documented policies, practices, procedures and related corporate documents;
- Review of committee documentation and Records of Decision (RoD); and
- A survey of employees with IM-related responsibilities.

The audit complied with accepted internal auditing practices and was conducted in accordance with TB Policy on Internal Audit.

3.0 OBSERVATIONS AND RECOMMENDATIONS

3.1 GOVERNANCE FRAMEWORK, STRUCTURE AND OVERSIGHT BODIES

The PPSC has fundamental elements of IM governance in place. However, improvements could strengthen the administration of IM oversight bodies.

The repatriation of IM services to headquarters from regions previously provided by the DoJ is having a positive effect on service delivery and office operations; however, there remains limited control and visibility over IM work in some regions. Expanding activities to monitor and report on IM is needed to support oversight and the identification of issues requiring corrective action.

We expected that the PPSC had implemented an appropriate governance structure and framework to adequately fulfill its IM objectives and activities.

Governance Framework and Oversight Bodies

We found fundamental elements of IM governance in place. The directorate has established three oversight bodies for the review and approval of IM policies, digital initiatives and plans: the Security and Digital Knowledge Management Committee (SDKC) serves as the departmental architecture review board with two newly created sub-working groups, the IM Working Group and the IM Out of the Box Working Group. Representatives from the IM function participate in these oversight bodies.

We reviewed RoDs and supporting documents of the three IM oversight bodies and found weaknesses in the following areas:

- Oversight bodies were meeting less often than prescribed in their Terms of Reference.
- The information captured in the records of decision for meetings were insufficient to assess whether oversight bodies were fulfilling all responsibilities prescribed in their mandates.
- There was no mandate for the IM Out of the Box Working Group.
- The SDKC was not explicitly receiving information or recommendations from the two working groups below it

- Insufficient information was available to conclude whether the SDKC was acting as an advisory body to the Executive Council relative to security, IT, IM and/or knowledge management.

Communications

In regions reporting to headquarters (British Columbia, Ontario, National Capital Region, and Saskatchewan), we found that IM management provided appropriate communication and information to support IM employees.

However, IM headquarters had limited communication and/or reporting in regions serviced by DoJ and/or with locally managed IM teams. We found the following concerns through interviews with IM senior management and employees:

- Management does not know how regions with local IM teams are handling information assets because they do not report to headquarters.
- Regions managed by DoJ are handling simple tasks such as mail services and the opening of files from the records room; however, they are not properly fulfilling lifecycle management responsibilities, which includes the retention and disposition of information.

Limited resources are also a concern. The lack of personnel is perceived by IM senior management to be the biggest risk to the PPSC in meeting its IM objectives and obligations. The organization does not have enough people to support more IM/IT awareness and training, which could increase the risk of inadvertent disclosure or loss of sensitive information.

IM Plans

We found no significant compliance issues in the alignment of strategic and operational IM plans with TB requirements. Plans were risk-based and considered the Department's strategic objectives, namely the continued implementation of two major foundational elements to its digital platform: Amicus and GCdocs.

However, the IM National Plan 2019-2022 did not account for short and long-term staffing issues or organizational funding constraints. For example, the IM National Plan projected hiring 30 new IM employees between 2019 and 2022. We reviewed new hires between 2019 and 2022 and found that less than half of the planned staffing had occurred. Interviews with IM senior management revealed that these plans were developed independently by members of IM management without feedback of key stakeholder's and regional representatives from oversight bodies and the plans have not been adjusted to reflect current realities.

Roles and Responsibilities

The PPSC has implemented the Directive on Information Management, defining the roles and responsibilities of employees, managers, IM personnel, and the CIO. Other PPSC documents establish similar IM roles and responsibilities for the management of protected and classified information, records disposition, and security guides. A contact page on iNet includes a list of all of key IM personnel at headquarters, as well as records management contacts in regions.

Despite documented roles and responsibilities, we found that IM services and standards were not consistently followed. We conducted a survey of 10 IM employees from regional offices and found that

all employees reported having a clear understanding of their IM roles and responsibilities. However, the same survey revealed that only two employees reported spending more than 50% of their time on IM-related activities. In the North: IM was a secondary task to performing other organizational functions; additional assistance and guidance was required when it came to disposition and the shipment of files to Iron Mountain; and there was uncertainty about the type of protected information in the offices. In regions managed by IM headquarters, such as Ontario and British Columbia, job titles and work descriptions more adequately reflected and aligned with job activities and responsibilities.

Policy Instruments

A review of PPSC policies, directives, and guidelines determined that they complied with TB requirements. The IM directorate documented and communicated its central IM policy instrument in the Directive on Information Management. The depth and breadth of associated IM policies, directives, and guidelines were appropriate.

However, we noted that the PPSC's central IM policy could be more aligned with the TB Directive on Open Government. The PPSC has not documented how its information and data are managed to enable data interoperability, reuse, and sharing to the greatest extent possible within and with other departments across the government.

Furthermore, policy instruments were not always dated. This is made it more difficult to know whether the policies were being kept current or for employees to know for certain that they were following the most current guidance.

Monitoring and Reporting

The DG, ASD and the Director, IM, reported that there is no IM monitoring framework in place at the PPSC. The IM program does not have the capacity to monitor whether employees are following internal and/or TB policies, directives and/or guidelines. Monitoring of IM actions and transactions is needed to support oversight of IM practices and the identification of issues requiring corrective action. In the absence of monitoring of PPSC's IM networks and activities, the organization may face reduced efficiencies, as well as increased costs and vulnerability to security threats.

Recommendations

The DG, ASD should strengthen oversight over information assets by implementing monitoring mechanisms to measure and provide regular reporting on activities related to information management.

3.2 SYSTEMS AND CONTROLS

The current IM framework provides guidance for information management throughout its life cycle and its directives align with TB policies relating to the management of information and technology. Despite this guidance, there is inconsistent application of measures to manage PPSC information assets.

We expected the PPSC to have implemented effective controls to manage information adequately and mitigate risks.

Record Keeping Practices

We found that the IM team established and published several reference documents on taxonomy, classification, and the identification and management of information of business value. This information is reinforced in a series of IM 101 videos on iNet for PPSC employees. However, there continues to be access issues with these videos links preventing employees from viewing the contents.

While the PPSC has a framework which provides direction and guidance to employees in headquarters and the regions, interviews with IM staff indicated that employees were not using established taxonomies and classification structures on a consistent basis.

It was reported that the storage of sensitive information varies from region to region, especially in regions where IM is not directly managed by headquarters. For example, in the Quebec Regional Office, it was reported that human resource (HR) files were being stored in openly accessible folders. Furthermore, management specified that IM employees were not always assigning the proper security level to prosecution files/documents and treating them accordingly. We found that there is a lack of IM awareness among PPSC employees on the different levels of security, and differences between confidential vs. business confidential information.

It was also stated that employees are not keeping documents in designated repositories. As noted above, there are not enough IM staff to monitor whether employees at headquarters and in the regions are using the taxonomies and classification structures correctly. The absence of regular monitoring threatens the confidentiality, integrity, and availability of the PPSC's information assets. Expanded monitoring would support oversight of IM practices and the identification of issues requiring corrective action.

We found that archiving of paper documents at the PPSC was done routinely. Concerns were reported, however, with DoJ sending active files to Iron Mountain for archiving when they should have remained on site and northern regions were not always archiving their information correctly. In response to these issues, IM management instituted management sign off prior to archiving of PPSC information.

The PPSC has negotiated with LAC to identify subsets of PPSC information that have archival value to Canada. More specifically, LAC wants to archive PPSC legal files related to indigenous homicides, dangerous and long-term offenders, as well as legal files related to Missing and Murdered Indigenous Women. Other files of interest are prosecution files before the Supreme Court of Canada.

In the absence of the PPSC being able to identify documents of archival interest to LAC, the Department risks losing or destroying records.

Systems and Tools

Electronic systems at the PPSC are the preferred means of creating, using, and managing information. It is important to note, however, that there remains a reliance on paper documents, and this is expected to continue, for court proceedings. Based on interviews with IM managers, the PPSC is unlikely to completely transition from paper to digital records as a result.

The implementation of GCdocs has been an important milestone for the PPSC in establishing a framework to manage information across the organization. However, adoption of GCdocs has not been consistent in all regions. Employees in northern offices still keep corporate information on the Shared Drive, P Drives, and/or their desktops because of low bandwidth. This information cannot be managed, or monitored, by IM at headquarters because the PPSC cannot manage information on the Shared Drives, which are owned by DoJ, or what is saved on a desktop.

Retention and Disposition

The PPSC has a Records Disposition Process in place, along with retention schedules, that are available on iNet. However, interviews with IM management consistently indicated that the disposition of records was not taking place at the PPSC. The lack of regular disposition activities results in $500,000 annually in paper storage costs for the organization; over time, this will also impact electronic storage costs. In addition, inefficiencies are likely because PPSC systems have to process more and more data, including in the context of responding to Access to Information and Privacy requests.

IM and Security Awareness

The IM and Security teams have dedicated IM and Security Awareness employees and training programs complemented by training offered by the Canada School of Public Service. A recent initiative by the Security team was the "The virtual escape room game" launched in January of 2022. It highlights infractions that were the most frequently identified in security sweeps and is accessible on every employee's desktop. However, it is not possible to track or determine how many employees have completed the game, thereby showing an increase in awareness.

IM managers were concerned about new hires not receiving sufficient IM training when they join the organization. The Director, IM would like to work with HR to identify new hires and provide direct training from the start. The IM team is also working on creating a more robust training program to enhance IM awareness across the organization.

The IM team is looking at new technologies as a means of disseminating more awareness to employees. The team is also developing content for the Information Management Awareness month in September and other training initiatives including in person learning, and training for staff when new technologies are rolled out.

Recommendations

The DG, ASD should ensure that a records disposition program is implemented to alleviate the financial impacts and minimise maintaining information that no longer has business value.

The DG, ASD should implement a systematic approach to identify and assess subsets of PPSC documents of archival value to Canada.

4.0 CONCLUSION

The IAED assessed the adequacy and effectiveness of the IM control framework against pre-established audit criteria based on TB policies, directives and guidance, PPSC policies, directives, and procedures, as well as general best practices.

Overall, the PPSC has appropriate governance structures and an IM framework for the management of PPSC's information assets throughout its life cycle that comply with TB policies. Despite this, the application of measures to manage PPSC information assets are performed inconsistently across the organization. Furthermore, the absence of an implemented monitoring framework prevents IM management from identifying gaps and taking mitigating actions.

IM plans and strategies should ensure consideration of short and long-term staffing issues as well as organizational funding constraints. Additional communication and training for employees would further improve overall efficiencies and compliance. The implementation of a monitoring framework is needed

to support oversight of IM practices and the identification of issues requiring corrective action. Strengthening the current records disposition program would alleviate data storage costs and minimise the amount of information the Department retains that no longer has business value. A systematic approach to identify and assess subsets of PPSC documents of archival value to Canada is needed to ensure the regular transfer of relevant documents to LAC.

5.0 MANAGEMENT ACTION PLANS

RECOMMENDATION	MANAGEMENT ACTION PLAN	OFFICE OF PRIMARY INTEREST	TARGET DATE
1. The DG, ASD should strengthen oversight over information assets by implementing monitoring mechanisms to measure and provide regular reporting on activities related to information management. *Risk: medium*	Management agrees with this recommendation. 1. To improve on oversight and resource availability: • Assess the need to repatriate salaries and the work from the Northern offices and provide the proposed solution to the Resource Management Committee for approval. • Repatriate funds from the Justice MOU for the Quebec and Atlantic regions • Hire permanent FTEs to support IM in the regions 2. Implement annual monitoring procedures scaled to PPSC risks and resources. 3. Report on the result of monitoring to the Senior Management Team on an annual basis. Areas requiring improvement will be tasked and follow-up will be done with management.	Director, Information Management & CDO	December 31, 2023
2. The DG, ASD should ensure that a records disposition program is implemented to alleviate the financial impacts and minimise maintaining information that no longer has business value. *Risk: medium*	Management agrees with this recommendation. 1. Seek permanent or temporary funding to hire FTEs to implement a disposition program/project to dispose of all PPSC information that has reached the end of the retention period. 2. If funding is not available, a disposition program will be developed based on risk and capacity. The program will be	Director, Information Management & CDO	March 31, 2024

RECOMMENDATION	MANAGEMENT ACTION PLAN	OFFICE OF PRIMARY INTEREST	TARGET DATE
	presented to Security, Digital and Knowledge Management Committee for approval.		
3. The DG, ASD should implement a systematic approach to identify and assess subsets of PPSC documents of archival value to Canada. *Risk: medium*	Management agrees with this recommendation. 1. Seek temporary funding to hire FTEs to identify PPSC's existing information of archival value and transfer to LAC and implement a systematic approach to identify and manage the information of archival value. 2. If funding is not available, an approach will be developed based on risk and capacity. The program will be presented to Security, Digital and Knowledge Management Committee for approval.	Director, Information Management & CDO	March 31, 2024

APPENDIX A – AUDIT CRITERIA

Audit Criteria
1. The Public Prosecution Service of Canada has implemented an information management structure to adequately fulfill its IM objectives and activities.
2. The Public Prosecution Service of Canada has implemented effective controls to manage information adequately and mitigate risks.

APPENDIX B - LIST OF ACRONYMS/ABBREVIATIONS

CIO	Chief Information Officer
DG, ASD	Director General, Administration Services Directorate
DoJ	Department of Justice
DPS	Digital Prosecution Strategy
HR	Human Resources
IAED	Internal Audit and Evaluation Division
IM	Information Management
LAC	Library and Archives Canada
PPSC	Public Prosecution Service of Canada
RoD	Records of Decision
SDKC	Security and Digital Knowledge Management Committee
TB	Treasury Board of Canada