Internal Audit Division

Audit of Information Technology

Final Audit Report

May 2016

Recommended for Approval to the Director of Public Prosecutions by the Departmental Audit Committee on May 3, 2016.

Approved by the Director of Public Prosecutions on May 5, 2016.

Canada

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY

1.1 AUDIT OBJECTIVE

The objective of this audit was to assess the adequacy and effectiveness of the governance structures, processes and controls to support the management of Information Technology (IT) resources and ensure compliance with the Treasury Board (TB) *Policy and Directive on the Management of Information Technology*.

The audit focused on the governance structures and strategic planning processes for IT, as well as the interfaces with the Corporate Service Provider (CSP) and the Government of Canada Service Provider (GCSP). The audit was carried out between October 2015 and February 2016. It included interviews with IT Management, members of the Information Management and Technology Committee (IMTC), and representatives from the CSP and GCSP. It also included a review and analysis of relevant IT documents.

1.2 AUDIT CONCLUSION

Overall, the audit found issues of moderate risk related to IT that need to be addressed in the areas of IT Governance, IT Roles and Responsibilities, IT Planning, IT Service Provider reporting, and IT Policies and compliance.

1.3 SUMMARY OF FINDINGS

During the audit, the following strengths were noted:

- The Information Management and Technology Committee (IMTC) has been created as a forum to discuss discrete IT operational issues.
- Roles and responsibilities between the Public Prosecution Service of Canada (PPSC), CSP and GCSP are clear.
- A corporate process is in place to manage IT risks.
- The relationships with the CSP and GCSP are improving.
- The PPSC intranet site contains useful IT-related guidance to staff.

This report includes the following recommendations addressed to the Deputy Director of Public Prosecution, Regulatory & Economic Prosecutions and Management Branch (DDPP,REPMB), in collaboration with the Director, Administration Services Division (ASD):

- Review the role and structure of the Chief Information Officer (CIO) organization, and make organizational changes necessary to meet the Treasury Board of Canada Secretariat (TBS) expectations of the role.
- Review the mandate and administration of the IMTC.

The report also includes the following recommendations addressed to the CIO:

- Establish a process to update the IT Plan to align with the requirements of the TB Directive on Management of Information Technology as well as the current needs of stakeholders throughout the organization.
- Request that the CSP and the GCSP service agreements with the PPSC include performance measures for the services rendered.
- Continue the review of IT policies to determine if PPSC IT policies are required, and clearly distinguish between IT policy requirements and guidance.
- Provide training and promote compliance to employees on IT policy requirements.

1.4 STATEMENT OF ASSURANCE

In my professional judgment as the PPSC's Chief Audit 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, against pre-established audit criteria that were agreed upon with the PPSC's management. The findings and conclusion are applicable only to the entity examined. The evidence was gathered in compliance with TB policy, directives, and standards on internal audit.

I appreciate the cooperation and assistance provided to the audit team by PPSC staff.

Julie Betts
Chief Audit Executive

2.0. INTRODUCTION

2.1. BACKGROUND

2014-15 Information Management and Information Technology Unit Overview[1]

Salary ($)	O&M ($)	Total ($)	FTEs
871, 566	2, 376, 965	3, 248, 531	10.37

The Information Management (IM) and Information Technology (IT) Unit consisted of 10.37 FTEs in 2014-15; currently there are 7.5 FTEs given recent departures. The Unit is currently led by the Manager of IM/IT and Chief Information Officer (CIO), and is part of the Administration Services Division within the REPMB.

The Unit provides IT management, IT support and other related services internally, and relies heavily on service providers for the provision of IT services. The PPSC has a Memorandum of Understanding (MOU) in place with the Corporate Service Provider (CSP) for the provision of various services including IT. PPSC also leverages the IT infrastructure provided by, and has numerous agreements in place with, the Government of Canada Service Provider (GCSP) for telecommunications and other IT services. In addition to basic email, file and print services, PPSC uses various applications including iCase – a web-based application that supports case management, time management and operational reporting; and GCDocs – an electronic document and records management system.

The Internal Audit Division conducted this audit of information technology in accordance with the PPSC's 2015-2018 Risk-Based Audit Plan, which was approved by the Director of Public Prosecutions on March 26th, 2015.

2.2. OBJECTIVES AND SCOPE

The objective of this audit was to assess the adequacy and effectiveness of the governance structures, processes and controls to support the management of IT resources and ensure compliance with the TB *Policy and Directive on the Management of Information Technology*.

The audit focused on the governance structures and strategic planning processes for IT, as well as the interfaces with the CSP and GCSP.

2.3. METHODOLOGY

The audit was performed in accordance with generally accepted auditing practices and was conducted in accordance with the TB *Policy on Internal Audit*.

[1] Public Prosecution Service of Canada's Financial Situation Summary Report as of March 31, 2015.

The audit methodology included the following:

- interviews with IT Management, members of the IMTC, and representatives of the CSP and the GCSP;
- a review and analysis of documented IT policies, practices and procedures, and related compliance documents;
- a review and analysis of IT governance-related committee terms of reference and meeting minutes;
- a review and analysis of IT planning, IT risk assessments and performance measurement-related documents; and,
- a review and analysis of IT service provider agreements and performance assessments.

The audit was carried out between October 2015 and February 2016.

3.0 OBSERVATIONS AND RECOMMENDATIONS

3.1 IT GOVERNANCE

The IMTC has acted as a forum to discuss discrete IT operational issues; however, the IMTC has not met on a regular basis, strategic level discussions have not occurred, and membership is not fully aligned with the mandate of the Committee.

The audit expected to find IT governance structures that are effective at defining an IT strategy and vision as well as providing timely oversight of IT investments.

The audit found that the IMTC is the main PPSC governance body for IT. It is a non-decision making body whose mandate is to provide oversight over IT, IM, and Knowledge Management (KM), and provide recommendations to Executive Council (EC), the senior committee to which the IMTC reports.

Committee Discussions

The audit found that the IMTC is a forum to discuss discrete IT operational issues, such as the use of USB keys and allocation of printers. However, a significant component of the mandate of IMTC is to provide recommendations to EC on an IT vision, direction or strategy and EC decisions have not benefited from IMTC advice. In addition, IMTC has not shared information with the Senior Advisory Board (SAB) as expected per its terms of reference. Lastly, the Performance Measurement Committee (PMC) has oversight for iCase-related matters however, the audit noted that information is not being shared between IMTC and PMC.

Per its terms of reference, the IMTC is to meet quarterly; however, the IMTC has only met once or twice per year in recent years.

If the IMTC does not fully meet its mandate by meeting regularly and providing recommendations to EC on an IT vision, direction and strategy, there is an increased risk that EC will not have the information required to develop the IT vision and strategy, which could lead to misalignment of IT investments and an increasing difficulty in meeting the IT needs of stakeholders. Similarly, if the IMTC does not share information with SAB and PMC, there is an increased risk of misalignment between the committees and IT investments.

Membership

It was also noted that the current Chair of the Committee, is the Manager of IM/IT and CIO,. The Manager is the most junior member of the Committee, which can prove challenging in terms of directing the work of the Committee. Interviews indicated that the role of the Manager is to focus on IT matters. If this occurs, the Manager may be less suited to Chair a Committee with a broader mandate encompassing IT, IM and KM, and increasing the risk that the IMTC will not be effective at carrying out its mandate.

Recommendation:

1. *The DDPP, REPMB should, in collaboration with the Director, ASD, review the mandate and the administration of the IMTC.*

3.2 ROLES AND RESPONSIBILITIES

Roles and responsibilities between PPSC and the service providers are clear; however, most PPSC IT work descriptions are out of date, the organization lacks IT strategic planning capacity, and the current CIO role is not currently aligned with TBS expectations.

The audit expected to find that roles and responsibilities related to IT were clearly defined and communicated.

The audit found that roles and responsibilities between the PPSC and the service providers are clear and have been documented; GCSP is responsible for managing the IT infrastructure (networks and data centers). The CSP provides various IT support services as detailed in the MOU.

The CIO role is currently assigned to the Manager of IM/IT. The expectation from the TB *Policy on Management of Information Technology* (section 6.1.6) is that: "A senior official is designated to represent the department in discussions with Treasury Board of Canada Secretariat (TBS) for the purposes of this policy". While the seniority of the official is not specified in the Policy, designated CIOs in departments of a similar size as the PPSC are within the EX classification. It should be noted however that these similarly sized organizations do not leverage IT service providers to the same extent as PPSC and consequently, have larger IT organizations internally.

The TBS has issued a CIO profile and other documents that clearly establish new expectations of the federal government department CIO as a "business enabler", evolving from service provider to strategic business partner and innovation agent. That shift was accentuated by the creation of GCSP, which took over the technical management of the IT infrastructure, enabling the CIOs to focus on business enablement and strategic planning. The current PPSC CIO's role is not currently aligned with the TBS CIO profile of new expectations.

Most IT work descriptions within the PPSC are outdated and do not reflect changing responsibilities since the creation of the GCSP or other IT organizational changes within the PPSC. In addition, IT strategic planning responsibilities are not specifically tied to any of the active job descriptions, and the Performance Management Agreement (PMA) of the Director of ASD, to whom the CIO organization now reports, does not currently contain any strategic objectives related to IT.

If the assignment of the CIO role and the focus of the CIO organization are not aligned with TBS expectations, there is an increased risk that the CIO organization will not adequately support business objectives, in addition to not being in compliance with TB policy instruments. If IT job

descriptions are out of date, there is an increased risk that roles will be unclear and that tasks will be performed in an inefficient and ineffective manner.

Recommendation:

2. *The DDPP, REPMB should, in collaboration with the Director, ASD, and the Human Resource Directorate, review the role and structure of the CIO organization including updating IT job descriptions and IT objectives in PMAs.*

3.3 IT PLANNING

The PPSC IT Plan has not been updated since 2014-15 and does not align with the TB *Policy on the Management of Information Technology,* nor is it supported by adequate performance measures.

The audit expected to find that an IT planning process was in place to identify and prioritize IT investments in line with the strategic objectives of the organization, and supported by an adequate IT risk management process and performance measurement process.

The audit found that the PPSC IT Plan was last updated in November 2013 for the 2014-15 fiscal year. The plan provides a table of IM/IT expenditures, total IM/IT budget, and a bulleted list of projects contemplated for 2014-15, but does not contain a number of the elements listed in Appendix B of the TB *Directive on the Management of Information Technology* such as: defining an IT strategy and planned investments for a five-year period, categorizing IT resource allocations, and defining IT performance measures.

Furthermore, the audit found that a process has not been put in place to gather input from stakeholders on their current and future needs (by leveraging the IMTC or through other means), and to help ensure that the plan reflects the business priorities of the organization as well as the current and future needs of stakeholders throughout the organization.

It was noted that the PPSC corporate risk management process considers IT related risks, amongst others. Specifically, the 2014-15 Corporate Risk Profile identifies a risk related to Information Management and Technology. The risk management process includes monitoring of the risk through action plans and annual status updates at EC and the Departmental Audit Committee.

If a strategic IT plan and IT visions are not in place, there is an increased risk that IT investments used to support the achievement of the objectives of the organization will not be identified or aligned with the needs of stakeholders.

Recommendation:

3. *The CIO should establish a process to update the IT Plan to align with the requirements of the TB Directive on the Management of Information Technology and the needs of stakeholders throughout the organization.*

3.4 IT SERVICE PROVIDERS

The relationships with the IT service providers are improving. They are managed through regular, informal bilateral meetings. Vendor performance reporting could be improved, and there is an opportunity to further leverage other clients to strengthen demands on GCSP.

The audit expected to find that an adequate process was in place to define measurable service expectations with IT service providers, that performance was measured on a regular basis, and that gaps in performance were being addressed in a timely manner.

The audit found that the relationship with the CSP is governed by an MOU, and managed through regular, informal bilateral meetings. Discussions on CSP performance also occur in the context of the annual renewal of the MOU, where adjustments may be made to better reflect the needs and performance of the parties. The PPSC IT management and the CSP representative have both confirmed that these meetings have helped improved the relationship.

The MOU with the CSP does not currently involve formal service levels beyond the acknowledgment that each party will seek to provide services to the other party in a similar manner as for internal services. While establishing formal service levels may be beyond the spirit of the MOU, it was noted that the CSP already has defined service levels internally with its own service provider for services which include IT support services provided to the PPSC; however, the PPSC does not currently have any presence on these established service levels.

Similarly, the relationship with the GCSP is governed by various agreements, and managed through regular, informal bilateral meetings. The PPSC IT management and the GCSP representative have both confirmed that these meetings have helped improve the relationship. Some of the agreements include provisions for GCSP to provide performance reports to the PPSC; however, to date these reports have not been formally requested[2].

In addition to bilateral meetings, the PPSC attends GCSP meetings with Heads of IT from other GCSP Clients[3] to discuss topics of common interest, including service level commitments. The 2015 Fall Report of the Auditor General of Canada on *Information Technology Shared Services* has also highlighted the GCSP challenges in establishing and meeting service expectations with its partners. There is an opportunity for the PPSC to further leverage the Heads of IT meetings and the common interests of clients to strengthen demands on the GCSP to commit to expected service levels.

If service level agreements are not established and performance reports are not obtained, the performance of service providers cannot be readily measured, and corrective actions become more difficult to implement.

[2] These reports would provide more tangible support to PPSC on whether service expectations are being met.
[3] Clients include those federal government organizations that procure services from or through GCSP, but are not part of the 43 large departments and agencies that are referred to as partners.

Recommendation:

4. *The CIO should request that the CSP and the GCSP service agreements with the PPSC include performance measures for the services rendered.*

3.5 IT POLICIES AND COMPLIANCE

The PPSC intranet contains useful IT-related guidance to staff, but it is not clear if the guidance consists of policy requirements or simply suggestions to staff. Some IT awareness is provided to staff, but no formal training on IT policy requirements. Compliance with IT policies is not formally monitored.

The audit expected to find that PPSC IT policies/directives are developed in alignment with TB policies, and that compliance with IT policy requirements was being monitored on a regular basis and corrective actions were being taken in a timely manner.

The audit found that the IT section of the PPSC intranet contains a number of pages with IT guidance related to topics such as network accounts, IT security, hardware and software, working remotely and other related topics. The guidance is useful for staff to understand how to better leverage technology in the context of their work. It is not always clear if the guidance constitutes policy requirements that staff must adhere to, or simply guidance for their consideration. The formal IT policy mentioned on the intranet is the *TB Policy on Acceptable Network and Device Use* from the CSP.

Interviews confirmed that the PPSC has not developed its own IT related policies, and that the organization is currently reviewing TB and CSP IT policies to determine if additional policies or guidance needs to be developed. The audit reviewed the intranet guidance currently available and found gaps such as IT security covering electronic disclosure.

Awareness of IT guidance is made available to employees from time to time through Intranet Bulletins, and a phishing simulation is ongoing to help promote IT security practices amongst staff; however, training or employee orientation on actual TBS, CSP or PPSC policy requirements has not been provided, and staff adherence to policy requirements is not monitored at all levels.

If IT policy requirements are not clearly identified and training is not provided to staff, there is an increased risk that staff will not comply with IT policy requirements. If PPSC-specific requirements are not developed where warranted, there is an increased risk that PPSC-specific IT requirements, including the management of electronic disclosures, will not be met.

Recommendations:

5. *The CIO should continue the review of IT policies to determine if PPSC IT policies (e.g. IT Security Policy) are required, and clearly distinguish between IT policy requirements and IT guidance.*

6. *The CIO should provide training and promote compliance to employees on IT policy requirements.*

4. CONCLUSION

The Internal Audit Division assessed the adequacy and effectiveness of governance structures, processes and controls to support the management of IT resources and ensure compliance with the TB *Policy and Directive on the Management of Information Technology*. Overall, the audit found issues of moderate risk related to IT that need to be addressed in the areas of IT governance, IT roles and responsibilities, IT Planning, IT service provider reporting, and IT policies and compliance.

4.0. MANAGEMENT ACTION PLAN

RECOMMENDATION	RISK LEVEL	MANAGEMENT RESPONSE AND ACTION PLAN	OFFICE OF PRIMARY INTEREST	PROJECT SCHEDULE
1. The DDPP, REPMB should, in collaboration with the Director, ASD, review the mandate and administration of the IMTC.	Moderate	Management agrees to review the mandate and Terms of Reference of the IMTC.	DDPP, REPMB Director, ASD	End of Q 4 – 2016-17
2. *The DDPP, REPMB should, in collaboration with the Director, ASD and Human Resource Directorate, review the role and structure of the CIO organization including updating IT job descriptions and IT objectives in PMAs.*	Moderate	Management agrees to review the role and structure of IT within the PPSC. This would include reviewing job descriptions and setting objectives for IT staff in their PMAs.	DDPP, REPMB Director, ASD	PMA objectives to be set in Q1; review to be completed by the end of Q 4, 2016-17.
3. The CIO should establish a process to update the IT Plan to align with the requirements of the TB Directive on the Management of Information Technology and the needs of stakeholders throughout the organization.	High	Management agrees to update the IT plan, in accordance with existing policies and PPSC needs.	CIO	End Q2, 2016-17
4. The CIO should request that the CSP and the GCSP service agreements with the PPSC include performance measures for the services rendered.	Moderate	Management agrees to request performance measures from service providers prior to signing any new service agreement.	CIO	Ongoing

RECOMMENDATION	RISK LEVEL	MANAGEMENT RESPONSE AND ACTION PLAN	OFFICE OF PRIMARY INTEREST	PROJECT SCHEDULE
5. *The CIO should continue the review of IT policies to determine if PPSC IT policies (e.g. IT security policy) are required, and clearly distinguish between IT policy requirements and IT guidance.*	Moderate	Management agrees to review IT policies from central agencies and service providers to determine applicability for the PPSC. A re-organization of the IT page on the INET site will clearly differentiate between policy requirements and guidelines.	CIO	Ongoing review of policies Q4 2016-17 for review of INET site.
6. *The CIO should provide training and promote compliance to employees on IT policy requirements.*	Moderate	Canada School of Public Service training on IT policy will be implemented for all staff on a mandatory basis.	CIO	Q1 2017-18 to complete mandatory training.

APPENDIX A – LINES OF INQUIRY AND AUDIT CRITERIA

Lines of enquiry are the broad subject headings describing areas determined to be the most productive for review during the Planning Phase of this audit. Each line of enquiry is accompanied by a set of audit criteria that will be used to assess compliance and the adequacy of practices.

Lines of Enquiry	Audit Criteria
1. IT Governance	1.1 IT Governance structures are effective at defining an IT strategy and vision and providing timely oversight of IT investments.
	1.2 Roles and responsibilities related to IT are clearly defined and communicated.
2. IT Planning	2.1 An IT planning process is in place to identify and prioritize IT investments in line with the strategic objectives of the organization.
	2.2 The IT Planning Process is supported by an adequate IT risk management process and performance measurement process.
3. IT Service Providers	3.1 An adequate process is in place to define measurable service expectations with IT service providers, performance is measured on a regular basis, and gaps in performance are addressed in a timely manner.
4. IT Policies and Compliance	4.1 IT Policies/Directives have been developed and comply with TB policies.
	4.2 Compliance with IT policy requirements is monitored on a regular basis and corrective actions are taken in a timely manner.

APPENDIX B - LIST OF ACRONYMS

ASD	Administration Services Division
CIO	Chief Information Officer
CSP	Corporate Service Provider
DDPP	Deputy Director of Public Prosecutions
EC	Executive Committee
FTE	Full Time Equivalent
GCSP	Government of Canada Service Provider
HOIT	Heads of Information Technology
IM	Information Management
IMTC	Information Management and Technology Committee
IT	Information Technology
KM	Knowledge Management
MOU	Memorandum of Understanding
O&M	Operations and Maintenance
PMA	Performance Management Agreement
PMC	Performance Management Committee
PPSC	Public Prosecution Service of Canada
REPMB	Regulatory & Economic Prosecutions and Management Branch
SAB	Senior Advisory Board
TB	Treasury Board
TBS	Treasury Board Secretariat