AUDIT OF CYBER SECURITY

Internal Audit and Evaluation Division

December 2025

Public Prosecution Service of Canada
Service des poursuites pénales du Canada

Canada

As recommended by the Departmental Audit Committee, subject to approval by the Director of Public Prosecutions, on December 11, 2025.
Approved by the Director of Public Prosecutions on December 22, 2025.

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. J79-39/2026E-PDF

ISBN: 978-0-660-97848-2

CONTENTS

EXECUTIVE SUMMARY

Background

For departments in the Government of Canada (GC), the responsibility for cyber security is shared between Shared Services Canada (SSC), the Communications Security Establishment Canada (CSE), the Treasury Board of Canada (TB), and the department. The Public Prosecution Service of Canada (PPSC) also relies on the Department of Justice (Justice Canada) for the management of several of their information technology (IT) security services, applications, database development services, and remote access services via a Memorandum of Understanding.

Part of the PPSC's Strategic Security Plan 2021-2024 was to have PPSC IT Operations and Security Services work to strengthen its IT security capabilities as cyber threats grow, including repatriating IT security services from Justice Canada and developing an IT security service that meets appropriate requirements.

Objectives

The objectives of this audit were to ensure:

a. IT Security governance and risk management processes are in place and meet GC policy framework requirements.
b. PPSC employees are trained and aware of cyber security measures.

Audit Conclusion

Generally, the PPSC's policies, procedures, and processes inform management of cyber security activities in the organization, including roles and responsibilities that are defined and aligned with internal roles and external partners. Improvements could be made to ensure device and system inventories are complete and contain information that could impact business objectives.

[REDACTED]

While there are elements of security awareness and training in the organization, gaps remain that can hinder the development of the PPSC's security awareness culture. These include low completion rates of mandatory training across the organization and tailored training based on roles and responsibilities for IT security and operations staff. Tailored training could be beneficial to ensure engagement, retention and skill development, especially as IT staff continue developing their capabilities.

Summary of Recommendations

1. The Senior Director General, Corporate Services, should ensure that the 2025-28 Departmental Security Plan is promptly finalized, approved, and available to PPSC employees. Periodic assessment of progress against the plan should be established.
2. The Senior Director General, Corporate Services, should ensure that device and system inventories are complete and maintained on a regular basis. Consideration should be given to ensuring the inventories contain information that could impact business objectives, such as device lifecycle management.
3. The Senior Director General, Corporate Services, should develop, document, and implement a comprehensive IT security risk management approach and plan, aligned with Canadian Centre for Cyber Security (CCCS) IT Security Risk Management: A Lifecycle Approach (ITSG-33) guidelines, that considers the following:
    - Processes for identifying and documenting cyber security risks at a departmental level;
    - Defined risk tolerance, ownership, and authority structures for managing those risks; and
    - Methodology for assessing risk (e.g. likelihood, severity, and impact).
4. The Senior Director General, Corporate Services, in collaboration with Human Resources, should establish and maintain a comprehensive mechanism to effectively monitor and ensure the timely completion of mandatory cyber security training requirements.

FINDINGS AND RECOMMENDATIONS

Governance

Policies, Procedures and Processes to manage PPSC Cyber Security

What Was Expected

We expected that processes and structures would be in place to inform, direct, and monitor the PPSC's activities which inform the management of cyber security risk.

Generally, the PPSC's policies, procedures, and processes inform management on cyber security activities in the organization, including roles and responsibilities that are defined and aligned with internal roles and external partners. The IT Security team at the PPSC generally relies on the CCCS' ITSG-33 as its guiding framework which outlines key IT security risk management activities that should be undertaken at both the departmental level as well as the information system level within GC organizations.

There is an established identification and authentication management process that uniquely identifies and authenticates individuals including several account monitoring procedures performed by IT security personnel. Processes are in place to ensure that users with access privileges are informed, approved, security screened, and have appropriate separation of duties.

Roles and responsibilities, including those of the Chief Information Officer (CIO), Chief Security Officer, and the Designated Official for Cyber Security, are documented through work descriptions and through internal documents such as the PPSC Operational CyberSecurity Guide, PPSC Directive on the Management of Administrative Privileges, and the Cyber Security Event Management Plan (CSEMP). A review of the individuals and groups assigned to administrator roles generally showed adequate separation of duties. Identified weaknesses were communicated to management.

At the time of the engagement, the 2025-28 Departmental Security Plan (DSP) was still in draft form, being actively reviewed, and had not been approved by the Director General (DG), Administration Services and CIO or the Deputy Head. The previous DSP has since expired. The draft version meets requirements of the TB Policy on Government Security. However, without an approved DSP, the organization may not be able to finalize and carry out their strategic plan which could lead to operational disruptions and/or inefficiencies.

Recommendation

1. The Senior Director General, Corporate Services, should ensure that the 2025-28 Departmental Security Plan is promptly finalized, approved, and available to PPSC employees. Periodic assessment of progress against the plan should be established

FINDINGS AND RECOMMENDATIONS

Governance (cont'd)

Why it is Important

Generally, the PPSC's policies, procedures, and processes inform management of cyber security activities in the organization including roles and responsibilities are defined and documented.

Improvements could be made to ensure completeness of information regarding physical devices and information systems. [REDACTED].

Finally, improvements could be made to ensure that users with privileged roles have adequate separation of duties such as ensuring that the same employee cannot both modify and review security features in Microsoft 365.

Response and Recovery Plans

Security controls such as, identification and authentication management, are defined, documented, and implemented to meet departmental IT security requirements and in accordance with TB requirements. However, the Business Continuity Plan (BCP) is not current, having been last updated in May 2019. This was prior to significant changes in telework due the Covid-19 pandemic and the Government of Canada's Hybrid Work model. Finally, while the draft DSP 2025-28 identifies the conduct of a business impact assessment and revision of the departmental business continuity plans, this work has not been completed.

The CSEMP was approved in July 2024 and outlines the PPSC's incident response activities and provides guidance to the PPSC Cyber and IT teams in the event of a cyber incident. However, both the CSEMP and BCP do not include a process for their testing or update; the BCP has not been tested since 2018. [REDACTED].

Device and Information Systems Inventories

Physical devices and information systems that enable the PPSC to achieve business objectives are generally identified and managed. While ITSG-33 provides flexibility to departments in determining the scope of documentation for information system and device inventories, improvements could be made to ensure that inventories are more effective through regular reviews and ensuring information gathered is complete.

The PPSC has documented an information system inventory that identifies over 70 systems operated by Justice Canada, SSC or PPSC with 20 systems under the PPSC's technical ownership. However, the inventory did not include technical ownership information which could lead to a lack of visibility for decision-making especially given the complexity of cyber security and IT responsibilities across the PPSC and its partners (e.g. SSC, Justice Canada). This gap was addressed following a request from the internal audit team, resulting in an updated inventory that now reflects the ownership information more accurately for those 70 systems. Regularly reviewing and maintaining system inventories, including details on technical ownership, could help establish clearer visibility into system ownership both internally and for the organizations providing IT services to the PPSC (e.g. SSC, Justice Canada).

While physical devices are inventoried, the PPSC could improve its inventories by ensuring the information is complete and consider including information such as serial numbers for computers and lifecycle status of devices and systems. Insufficient information about devices could impact timely and accurate decision-making and lead to an increased risk of operational impacts on the PPSC.

Recommendation

2. The Senior Director General, Corporate Services, should ensure that device and system inventories are complete and maintained on a regular basis. Consideration should be given to ensuring the inventories contain information that could impact business objectives, such as device lifecycle management.

FINDINGS AND RECOMMENDATIONS

Risk Management and Assessment

What Was Expected

We expected to find that the PPSC understands its cyber security risks to operations, assets, and individuals. We also expected to find that the PPSC established its priorities, constraints, risk tolerances, and assumptions and used them to support operational risk decisions.

Overall, the PPSC's risk management for cyber security is in an immature state. While IT Security is working toward the development of a Governance and Risk Management Framework, there is currently no timeline for implementation.

The Policy on Government Security requires security risk governance, including responsibilities for security controls and authorities for security risk management decisions, be established. [REDACTED]. [REDACTED]. Establishing and documenting roles and responsibilities regarding risk management, including the determination of risk tolerance, could help clarify the accountability for providing this guidance.

[REDACTED]. While ITSG-33 is used as a reference, key components such as the development and implementation of security controls, documenting an overall risk register, and process mapping aligned with the guidance, remain in early stages. These activities are considered long-term initiatives, with timelines exceeding one year, primarily due to resource constraints (i.e. 1.5 dedicated employees) and shifting priorities.

FINDINGS AND RECOMMENDATIONS

Risk Management and Assessment

Why it is Important

[REDACTED].

[REDACTED]. This may lead to a reconsideration of the system's approved authority to operate.

While often at a high level, there is evidence that threats, vulnerabilities, impact, and sufficiency of controls are considered and documented to determine risk in the Security Assessment and Authorization (SA&A) process. Some improvements could be made to more thoroughly document the elements of the risk assessments (e.g. impact statement, sufficiency of controls, likelihood, rating methodology).

Recommendations, responses, and mitigation actions for residual risks identified in the SA&A process are documented in a Plan of Action and Milestones to obtain the Authority to Operate the system. The Authority to Operate is granted with the expectation that residual risks will be appropriately mitigated. While some elements have been put in place, significant resource constraints as well as shifting priorities mean that several recommendations and mitigation steps have not been addressed in the prescribed time.

[REDACTED].

Recommendation

3. The Senior Director General, Corporate Services, should develop, document, and implement a comprehensive IT security risk management approach and plan, aligned with CCCS' ITSG-33 guidelines, that considers the following:
    - Processes for identifying and documenting cyber security risks at a departmental level;
    - Defined risk tolerance, ownership, and authority structures for managing those risks; and
    - Methodology for assessing risk (e.g. likelihood, severity, and impact).

FINDINGS AND RECOMMENDATIONS

Training and Awareness

What Was Expected

We expected the PPSC to have a culture of security awareness supported by tailored awareness and training that is frequently reviewed, maintained and accessible to all users with access to departmental systems.

Why it is Important

While there are elements of security awareness and training in the organization, gaps remain that can hinder the development of the PPSC's security awareness culture. These include low completion rates for mandatory training across the organization and tailored training based on roles and responsibilities for IT security and operations staff. Tailored training could be beneficial to ensure engagement, retention and skill development, especially as IT staff are still developing their capabilities.

The PPSC does not have a security awareness and training policy nor an IT security awareness and training plan in place. In the absence of an IT Security awareness and training program, training based on current user-related vulnerabilities and proper use behaviours is conducted on an ad-hoc basis in addition to two mandatory courses for all PPSC employees.

These two courses are Discover Cyber Security (DDN235) and Security Awareness (COR310), both provided by the Canada School of Public Service at no cost. A data review revealed low completion rates for both courses with only 52% and 65% of participants, respectively.

The PPSC generally provides employees with information related to security awareness, including guidance on when and how to report security incidents. The information is primarily made available through the intranet and through an internal newsletter.

A phishing scam campaign was conducted by the PPSC's IT team in March 2025; however, shifting priorities have caused delays in analyzing the data.

Finally, we found that the SA&A process for Microsoft 365 identified the lack of a security awareness training program as a risk area. In addition, training gaps were identified among IT security and operations staff following the PPSC's undertaking of new IT responsibilities and limited experience in certain areas. As a result, mandatory training was identified to address these deficiencies. Upon review of the completion certificates, we found that of four employees working on cyber security, [REDACTED].

Recommendation

4. The Senior Director General, Corporate Services, in collaboration with Human Resources, should establish and maintain a comprehensive mechanism to effectively monitor and ensure the timely completion of mandatory cyber security training requirements.

MANAGEMENT ACTION PLANS

No.	Recommendation	Risk	Management Action Plan	Office of Primary Interest	Target Date
1	The Senior Director General, Corporate Services, should ensure that the 2025-28 Departmental Security Plan is promptly finalized, approved, and available to PPSC employees. Periodic assessment of progress against the plan should be established.	Medium	Management agrees with this recommendation. The SDG will determine the method of approval for the Departmental Security Plan and then it will be put forward for approval. It will be posted on iNet. A schedule will be determined for reporting progress to the Senior Management Team.	DG, ASD	January 31, 2026
2	The Senior Director General, Corporate Services, should ensure that device and system inventories are complete and maintained on a regular basis. Consideration should be given to ensuring the inventories contain information that could impact business objectives, such as device lifecycle management.	Medium	Management agrees with this recommendation. At this point, we have an inventory of laptops and cellphones that are managed by the department. We will look at adding some additional information for new devices. Adding this information for existing devices would be more work than we are staffed for.	Director, IT	March 31, 2026
3	The Senior Director General, Corporate Services, should develop, document, and implement a comprehensive IT security risk management approach and plan, aligned with CCCS' ITSG-33 guidelines, that considers the following: • Processes for identifying and documenting cyber security risks at a departmental level; • Defined risk tolerance, ownership, and authority structures for managing those risks; and • Methodology for assessing risk (e.g. likelihood, severity, and impact).	Medium	Management agrees with this recommendation. We will develop a comprehensive IT security risk management approach and plan. Progress on this will be slow due to lack of resources.	Director, IT	March 31, 2027
4	The Senior Director General, Corporate Services, in collaboration with Human Resources, should establish and maintain a comprehensive mechanism to effectively monitor and ensure the timely completion of mandatory cyber security training requirements.	Medium	Management agrees with this recommendation. Human Resources (HR) will work with Senior Management to add an indicator to executives' performance agreements regarding the completion of mandatory training by their staff. In addition, HR will send a list once a year to managers of their team's outstanding mandatory training.	Director, HR	July 31, 2026

APPENDIX A – AUDIT INFORMATION

Statement of Assurance

The audit was conducted in conformance with the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing and with the Treasury Board Policy and Directive on Internal Audit as supported by the results of the external quality assurance assessment.

Scope

The audit focused on the PPSC's controls and processes and excluded areas where our service provider, Justice Canada, is the business owner according to the Memorandum of Understanding.

Methodology

The review methodology included:

- interviews with various stakeholders, and,
- review and analysis of documented policies, practices, procedures, and directives related to cyber security.

Lines of Enquiry

1	Governance
2	Risk Management
3	Awareness and Training

APPENDIX B – LIST OF ACRONYMS/ABBREVIATIONS

BCP	Business Continuity Plan
CCCS	Canadian Centre for Cyber Security
CIO	Chief Information Officer
CSEMP	Cyber Security Event Management Plan
DSP	Departmental Security Plan
GC	Government of Canada
HR	Human Resources
IT	Information Technology
ITSG-33	IT security risk management: A lifecycle approach
Justice Canada	Department of Justice
PPSC	Public Prosecution Service of Canada
SA&A	Security Assessment and Authorization
SSC	Shared Services Canada
TB	Treasury Board of Canada