Internal Audit – Patch Management

Final Report

Audit, Evaluation, and Risk Branch

Canada Revenue Agency | Agence du revenu du Canada

Canada

© His Majesty the King in Right of Canada, represented by the Minister of National Revenue, 2026

Catalogue No. Rv4-229/2026E-PDF

ISBN 978-0-662-72478-0

This document is available on the Government of Canada website at www.canada.ca

This document is available in alternative Formats upon request

Table of contents

Executive summary **3**
Summary of recommendations 4
Management response 4
Introduction **5**
Focus of the internal audit **6**
Importance 6
Objective 6
Scope 6
Internal audit criteria and methodology 7
Findings, recommendations, and action plans **7**
Compliance 7
Monitoring and reporting 15
Acknowledgement **16**
Appendices **17**
Appendix A: Internal audit criteria and methodology 17
Appendix B: Glossary 18

Executive summary

Cyber security practices are fundamental to the Canada Revenue Agency's (CRA) ability to carry out its mandate of administering tax, benefits, and related programs, and to ensure compliance on behalf of governments across Canada. Gaps in cyber security systems and delays in responding to vulnerabilities increase the likelihood that cyberattacks may succeed, which could result in the theft of sensitive information and affect the delivery of programs and services to Canadians.

As part of the cyber security framework, patch management is one of many key practices to help prevent compromises, data breaches, operational disruptions, and adverse events. Patch management is the process of identifying, prioritizing, acquiring, installing, and verifying the installation of patches (also known as "repair jobs" or "fixes" for a piece of programming), updates, and upgrades throughout an organization.

Patch management is a shared responsibility within the CRA in coordination with lead security agencies in the Government of Canada. Within the CRA, the Security Branch (SB) is responsible for managing cyber security threats, cyber vulnerabilities, and cyber security events that would compromise networks and systems. The Information Technology Branch (ITB) is responsible for acquiring, testing, prioritizing, deploying, and verifying patches across the CRA, along with overseeing patch schedules and deployment performance.

The objective of the internal audit was to provide the Commissioner, CRA management, and the Board of Management with assurance that the CRA is patching security vulnerabilities in its systems and applications in a timely and effective manner.

Overall, the internal audit team concluded that corporate policy instruments are in place and patches are deployed to address critical and high-risk vulnerabilities. [redacted content]

The internal audit team found that:

- corporate policy instruments related to patch management are formally defined, current, and communicated
- [redacted content]
- [redacted content]

- [redacted content]

Summary of recommendations

[redacted content]



Management response

The SB and the ITB agree with the recommendations in this report and have developed related action plans. The Audit, Evaluation, and Risk Branch has determined that the action plans appear reasonable to address the recommendations.

Introduction

Cyber security practices are fundamental to the Canada Revenue Agency's (CRA) ability to carry out its mandate as Canadians must trust the CRA to protect their sensitive information. According to the National Cyber Threat Assessment 2025-2026[1], cyber threats, such as nation-state actors and cybercriminals, continuously search for exploits and are evolving in sophistication with artificial intelligence. Gaps in cyber security systems and delays in responding to vulnerabilities increase the likelihood that cyberattacks may succeed, which could result in the theft of sensitive information and affect the delivery of programs and services to Canadians.

As part of the cyber security framework, patch management is one of many key practices to help prevent compromises, data breaches, operational disruptions, and adverse events. Patch management is the process of identifying, prioritizing, acquiring, installing, and verifying the installation of patches (also known as "repair jobs" or "fixes" for a piece of programming), updates, and upgrades throughout an organization[2].

Patch management is a shared responsibility within the CRA, in coordination with lead security agencies in the Government of Canada.

Within the CRA, the Security Branch's (SB) mandate is to enable the seamless delivery of the CRA's programs and services by ensuring the protection of its people, information, and assets. The SB is responsible for managing cyber security threats, cyber vulnerabilities, and cyber security events that would compromise networks and systems.

The Information Technology Branch (ITB) develops, operates, and maintains the CRA's information technology (IT) and is responsible for acquiring, testing, prioritizing, deploying, and verifying patches across the CRA, along with overseeing patch schedules and deployment performance.

The CRA also coordinates security-related activities with Government of Canada lead security agencies and partners. The Treasury Board of Canada Secretariat, Communications Security Establishment, and the Canadian Centre for Cyber Security provide leadership, advice, and guidance related to protecting government IT infrastructure and systems. Shared Services Canada is responsible for the planning,

[1] National Cyber Threat Assessment 2025-2026 – Canadian Centre for Cyber Security, https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026

[2] NIST SP 800-40 Rev. 4 Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology, https://csrc.nist.gov/pubs/sp/800/40/r4/final

designing, building, operating, and maintenance of effective, efficient, and responsive IT infrastructure and services to secure CRA networks and systems[3].

These organizations work together to prevent data theft and limit disruptions to systems that deliver programs and services to Canadians. Guidance from both the Treasury Board of Canada Secretariat and the Canadian Centre for Cyber Security prioritizes patching operating systems and applications as one of the most important IT security actions and provides best-practice frameworks to support government organizations.[4,5]

Focus of the internal audit

This internal audit was included in the 2024-2025 Risk-Based Assurance and Advisory Plan, which was approved by the Board of Management on September 16, 2024. The Assignment Planning Memorandum was approved by the Commissioner on June 18, 2025.

Importance

An effective patch management process is a critical component of an organization's cyber security posture, ensuring that vulnerabilities are promptly addressed to reduce the window of opportunity for exploitation.

This internal audit provides assurance that key controls over the patch management process are in place and working as intended. The internal audit supports SB and ITB senior management by providing insights and recommendations to strengthen their patch management process.

Objective

The objective of the internal audit was to provide the Commissioner, CRA management, and the Board of Management with assurance that the CRA is patching security vulnerabilities in its systems and applications in a timely and effective manner.

Scope

The internal audit covered critical production systems, applications, endpoint devices, supporting processes, and activities. The period covered in this internal audit was from

---

[3] 2025 Report of the Auditor General of Canada to the Parliament of Canada, Cyber Security of Government Networks and Systems, https://www.oag-bvg.gc.ca/internet/English/parl_oag_202510_04_e_44720.html

[4] Top 10 IT security actions, https://www.cyber.gc.ca/en/guidance/top-10-it-security-actions

[5] Patch Management Guidance, https://www.canada.ca/en/government/system/digital-government/online-security-privacy/cyber-security-guidance-policy/patch-management-guidance.html

January 1, 2023, to December 31, 2024, but also considered the most recent activity, when relevant.

The management of infrastructure assets, such as mainframes, servers, networks under the responsibility of Shared Services Canada, and cloud services were outside the scope of this internal audit.

Internal audit criteria and methodology

The internal audit criteria and methodology can be found in Appendix A.

The examination phase of the internal audit took place from May 2025 to September 2025.

The internal audit was conducted in accordance with the Global Internal Audit Standards, as supported by the results of the quality assurance and improvement program.

Findings, recommendations, and action plans

The recommendations presented in this report address issues of high significance or mandatory requirements.

The SB and the ITB agree with the recommendations in this report and have developed related action plans. The Audit, Evaluation, and Risk Branch (AERB) has determined that the action plans appear reasonable to address the recommendations.

Compliance

Corporate policy instruments related to patch management are formally defined, current, and communicated.

Background

The internal audit expected to find that corporate policy instruments related to patch management requirements were documented, current, and published for communication to stakeholders.

Findings

The internal audit found that the CRA's corporate policy instruments are established, up to date, and approved. The Systems Hardening and Security Patch Management Standards define requirements for patch deployment timelines, risk-based prioritization, and exception/variance handling. The internal audit team noted that the Q4 2024-2025 changes to the requirements for timelines for patch deployment reflect the recent

changes made in the Canadian Centre for Cyber Security's and the Treasury Board of Canada Secretariat's guidelines on emergency patching requirements and timeframe alignment. The standards are published and accessible through internal websites for CRA staff.

Why it matters

Defined and clear policies for effective security and patch management strengthen decision making and ensure that stakeholders align with organizational objectives.

[redacted content]

Background

The internal audit expected to find a process in place for:

- [redacted content]
- [redacted content]

Findings

[redacted content]

[redacted content]

[redacted]

[redacted]

Why it matters

[redacted content]

Recommendation #1

[redacted content]

- [redacted]

Management response:

[redacted content]

Management response and action plan #1a:

[redacted content]

- [redacted]

[redacted content]

Management response and action plan #1b:

[redacted content]

Management response and action plan #1c:

[redacted content]

Management response and action plan #1d:

[redacted content]

[redacted content]

Background

The internal audit expected to find that patches were:

- [redacted content]
- [redacted content]
- [redacted content]

Findings

[redacted content]

[redacted content]

Why it matters

[redacted content]

Recommendation #2

The ITB, in consultation with the SB, should:

[redacted content]

Management response and action plan #2a:

[redacted content]

Management response and action plan #2b and #2c:

[redacted content]

[redacted content]

Management response and action plan #2d:

[redacted content]

Management response and action plan #2e:

[redacted content]

[redacted content]

Monitoring and reporting

[redacted content]

Background

The internal audit expected to find that performance indicators provided accurate and relevant information to support decision making related to patch management performance within the CRA and were reported to senior management.

Findings

The internal audit found that performance indicators were defined in the ITB's Branch Executive Committee reporting dashboards, and that patch activities were being monitored. [redacted content]

Why it matters

[redacted content]

Recommendation #3

[redacted content]

Management response and action plan #3

[redacted content]

Acknowledgement

In closing, the AERB would like to acknowledge and thank the SB and the ITB for the time dedicated and the information provided during the course of this engagement.

Appendices

Appendix A: Internal audit criteria and methodology

Internal audit criteria

Based on the AERB's risk assessment, the following lines of enquiry were identified:

Lines of enquiry	Criteria
1. Compliance	1.1 CRA policies, directives, standards, and procedures, including governance, related to patch management are defined, current, and communicated to stakeholders.
	1.2 Risk management approaches and information are used to assess and prioritize patches for systems and applications.
	1.3 Patches are prepared and deployed in compliance with policies and procedures.
2. Monitoring and reporting	2.1 Patch management performance indicators provide accurate and relevant information to support decision making.

Internal audit methodology

The methodology for examination included the following:

- reviewed and analyzed corporate policy instruments and supporting documentation related to patch management
- conducted interviews and walkthroughs with SB and ITB management and staff
- tested for compliance of controls through documentation reviews
- reviewed and analyzed data from supporting applications and tools
- reviewed and analyzed performance indicators and monitoring reports in place related to patch management

Appendix B: Glossary

Term	Definition
Common Vulnerabilities and Exposures	A database that provides unique identifiers for publicly known cyber security vulnerabilities.
Control	The means by which an organization reduces the likelihood of a risk occurring or the impact if it does. A control should be either preventative, detective, or corrective, and either manual or automated (i.e., system) in nature.
Cyberattack	The use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device.
Cyber security	The protection of digital information and the preservation of the integrity of the infrastructure that houses and transmits digital information. More specifically, cyber security includes the body of technologies, processes, practices, and response and mitigation measures designed to protect networks, computers, programs, and information from attack, damage, or unauthorized access to ensure confidentiality, integrity, and availability.
Cyber threat	A threat actor, using the Internet, who takes advantage of a known vulnerability in a product for the purposes of exploiting a network and the information the network carries.
Endpoint	Physical devices that connect to and exchange information with a computer network. Examples include mobile devices, desktop computers, virtual machines, embedded devices, and servers.
Enterprise application	An application built by the CRA's ITB according to their enterprise development process.
Exploit	A software tool, script, or code designed to take advantage of one or more vulnerabilities in software, firmware, or hardware that may jeopardize CRA data or systems.

Library	A collection of files, programs, routines, scripts, or functions that can be referenced in the programming code.
Mitigate	Included here to further re-enforce the notion that the requirement to mitigate a software vulnerability risk is not the same as fixing it. Whatever shortcoming, failure, or fault that has led to the identification of a vulnerability, the risk that the CRA may experience a related incident is reduced by mitigating actions while plans are made and carried out to resolve the root problem.
Non-certified library	A library not registered or with no other versions certified in the authoritative registry of all software and reusable components used in the CRA.
Patch	A “repair job” for a piece of programming; also known as a “fix.” A patch is the immediate solution to an identified problem that is provided to users; it can sometimes be downloaded from the software maker’s website.
Security control	A management, operational, or technical high-level security requirement needed for an information system to protect the confidentiality, integrity, and availability of its IT assets. Security controls can be applied using a variety of security solutions, including security products, security policies, security practices, and security procedures.
Security posture	An organization’s overall readiness to defend against cyber threats, including tools, policies, training, and response plans—everything that contributes to an organizations’ ability to spot, block, and bounce back from attacks.
Threat and risk assessment	The process of identifying physical assets within a facility or IT assets within a system, and assessing how these assets can be compromised, assessing the level of risk that threats pose to these assets, and recommending security measures to mitigate threats.
Vulnerability	A flaw or weakness in the design or implementation of an information system or its environment that could be exploited to adversely affect an organization’s assets or operations.