Canada Border Services Agency | Agence des services frontaliers du Canada

Canada

Audit of cyber security

Canada Border Services Agency

Agence des services frontaliers du Canada

Aussi disponible en français sous le titre :
Vérification de la cybersécurité

Audit of cyber security

Internal Audit and Program Evaluation Directorate
September 2025

Note: [redacted] appears where sensitive information has been removed in accordance with the *Access to Information Act* and the *Privacy Act*.

Table of contents

Introduction

Canadians rely on the Government of Canada (GC) to deliver programs and services that are essential to the health, safety, security and economic well-being of Canadians. The increasing digital presence of the GC and its reliance on information technologies to deliver programs and services means that federal departments and agencies are attractive targets for cyber threats or attacks. Due to the sensitive and confidential nature of information managed by the Canada Border Services Agency (CBSA or the agency), as well as its high operational value, cyber security events can have a significant impact on the agency's operations, either through the disruption of critical and essential services or through the exposure of classified, protected or personal information.

The Recourse, Standards and Program Integrity Branch (RSPIB), in collaboration with the Information, Science and Technology Branch's (ISTB), administers the CBSA Security Program, which includes cyber security. This program establishes governance, controls, practices and assurance to help the agency meet its obligations under the Policy on Government Security (PGS), and support the safe delivery of CBSA and GC programs, services and priorities.

In April 2024, a Cyber Security Directorate (CSD) was established within ISTB through a realignment of existing functions to further build capacity and advance the agency's cyber security priorities. The creation of the CSD formally integrated and expanded on several cyber security-related functions that were already housed within ISTB, providing a more unified structure to support the development, management, and oversight of the agency's cyber security program.

The CSD's key responsibilities include:

- Cyber security operations (incident response (IR), monitoring and vulnerability management)
- Risk management, assessment and compliance
- Security solution (architecture, engineering and integration)
- Cyber security program management (planning, governance, standards and reporting)
- IT continuity (contributing to the agency Business Continuity Plan)

About the audit

The objective of this audit was to assess whether the CBSA cyber security program had implemented an effective management control framework to support its objectives and mitigate cyber security threats/incidents.

Audit scope inclusions

The period under review spanned April 1, 2023 to March 31, 2025. Within that timeframe, the scope of work included the examination of cyber security governance, risk management and controls focusing on cyber security:

- roles and responsibilities within the agency
- plans to address cyber security risks
- event management processes
- awareness and training

Audit scope exclusions

The audit scope excluded the following:

- information management (including sharing of information with third parties)
- cyber security related activities performed by third parties (for example, Canada Revenue Agency (CRA) and Shared Services Canada (SSC)
- configuration management and change control
- physical security of IT assets

Note: During the review period of the audit, the GC's Enterprise Cyber Security Strategy was published, including a target operating model, therefore alignment to this whole-of-government approach was in progress and could not be evaluated.

Audit methodology

- 240+ supporting documents reviewed
- 60+ stakeholders interviewed
- 11 completed walkthroughs with stakeholders who played a key role in cyber security IR activities
- 2 audit tests performed on processes related to cyber security event management, including vulnerability and security patch management

Significance of the audit

An effective cyber security program relies on strong governance and well-defined management practices to prevent, detect, and respond to cyber vulnerabilities, threats, and incidents. Foundational elements such as risk management, oversight, and performance monitoring are critical to enabling a cyber security program that supports the agency's operational resilience and strengthens its overall security posture. Without them, the agency is at risk of increased exposure to disruptions, data breaches and ineffective threat responses which could jeopardize its digital infrastructure and sensitive information holdings.

An evolving cyber threat landscape, the agency's reliance on external stakeholders for critical IT services, and recent realignments within the ISTB highlight the increased need for well-defined roles, responsibilities and robust governance structure.

As a result, this Audit was approved as part of the 2024 to 2025 Risk-Based Audit Plan.

Statement of conformance

This audit engagement conforms to the Treasury Board's *Policy* and *Directive on Internal Audit* and the Institute of Internal Auditors' (IIA) *Global Internal Audit Standards*. Sufficient and appropriate evidence was gathered through various procedures to provide an audit level of assurance. The agency's internal audit function is independent, and internal auditors performed their work with objectivity as defined by the IIA's *Global Internal Audit Standards*.

Audit conclusion

A cyber security program plays a critical role in supporting the secure delivery of programs and services. As the program matures, it enhances the organization's ability to manage cyber security risks effectively and maintain operational resilience in response to the evolving threat environment.

The agency has built upon its existing cyber security functions by establishing a dedicated directorate. However, several known gaps remain that pose risks to the program's overall effectiveness. Accelerated efforts are needed to address these areas of concern. Further advancing the cyber security program—through finalization and consistent application of strategies, plans, policy instruments and procedures; clarification of roles and responsibilities; and the integration of regular oversight practices—will enhance program maturity and effectiveness.

Given that cyber security is one component of the broader departmental security portfolio, it is important that governance bodies and security functions collaborate to manage risks in a coordinated and holistic manner. Sustained and timely progress in strengthening cyber security governance, risk management and control functions, while fostering greater coordination across security-related responsibilities, will be critical to ensuring a more mature and resilient cyber security posture for the agency.

Summary of recommendations

1. [redacted]
2. [redacted]
3. Enhancing awareness and training through tailored content and regular effectiveness assessments to support continuous improvement

Management response

The Vice-President (VP) of ISTB welcomes the findings of the Audit of Cyber Security, has acknowledged and accepted the recommendations presented, and understands the importance of strengthening the agency's cyber security posture in order to protect the confidentiality, integrity, and availability of its information and IT assets. The ISTB is actively engaged in efforts to implement these recommendations, working both independently and in collaboration with other relevant parties in the agency and external stakeholders. [redacted]. The results of this audit and the CMSA will better inform the multi-year strategy the CSD is working on to improve the cyber security posture of the CBSA. The target completion of activities reflects what can be achieved based on the current complement of talent on strength. Should there be changes in the workforce capacity, the completion could accelerate.

Audit findings

The audit resulted in the findings below.

Cyber security governance and risk management

The agency is expected to have established a structured and integrated approach to cyber security. This includes defining, documenting, implementing and maintaining appropriate security controls, as well as developing policy instruments to support timely and coordinated responses to cyber security events. A robust cyber security approach also requires a risk management framework that incorporates proactive threat monitoring and supports decision making to ensure that operational-level risks are effectively monitored and used to inform broader departmental security planning.

These expectations are based on key GC policy instruments that outline requirements for departmental security, digital service delivery, and cyber event management, including the PGS, the Directive on Security Management, the Policy and associated Directive on Service and Digital, and the GC Cyber Security Event Management Plan (CSEMP). The GC's Enterprise Cyber Security Strategy further reinforces these expectations by outlining the need for departments to adopt a risk-based approach,

enhance collaboration among departments, reduce redundancies and strengthen the security and resilience of digital government services.

[redacted]

[redacted]

Recommendation 1

[redacted]

Management response: ISTB agrees with the recommendation and with the importance of strengthening the agency's governance around its cyber security program.

[redacted]

Completion date: September 2026

Policy instruments and strategy

Under the leadership of the CBSA Chief Security Officer (CSO) and Designated Official for Cyber Security (DOCS), the agency has developed eight security policies and a series of related directives and guidance in alignment with Treasury Board requirements on government security. Collectively, these policies are known as the CBSA Security Volume. The Volume is readily available on the agency's intranet, and most of its cyber security content was updated in 2024 to 2025.

Since its establishment, the new CSD has initiated efforts to develop cyber security policy instruments and strategies required for its key functions. These initiatives, which aim to strengthen governance, risk management, and control measures, were at various stages of development at the time of the audit. Some were still in draft form, while others had been finalized and approved. For example:

[redacted]

Internal stakeholders

Cyber security is a shared responsibility across the agency. While many units within ISTB and across the agency contributed to cyber security activities, whether directly or indirectly, the key internal stakeholders with primary responsibilities in this area were the CSD within ISTB and the Security and Professional Standards Directorate (SPSD) within RSPIB. The CSD operated under the DOCS, who was primarily responsible and accountable for cyber security, while the SPSD reported to the CSO, who was accountable for the overall departmental security. As such, the DOCS and the CSO roles are interdependent and require coordination to support the agency's overall security posture.

[redacted]

The CBSA Framework on Security Program Management outlined security responsibilities and accountabilities of key stakeholders. An agreement was signed in November 2021 to clarify functional roles and responsibilities for cyber security, as follows:

- VP ISTB, who is also the agency's Chief Information Officer, retains accountability for IT and cyber security
- Director General SPSD, who is also the agency's CSO, is accountable for information management security

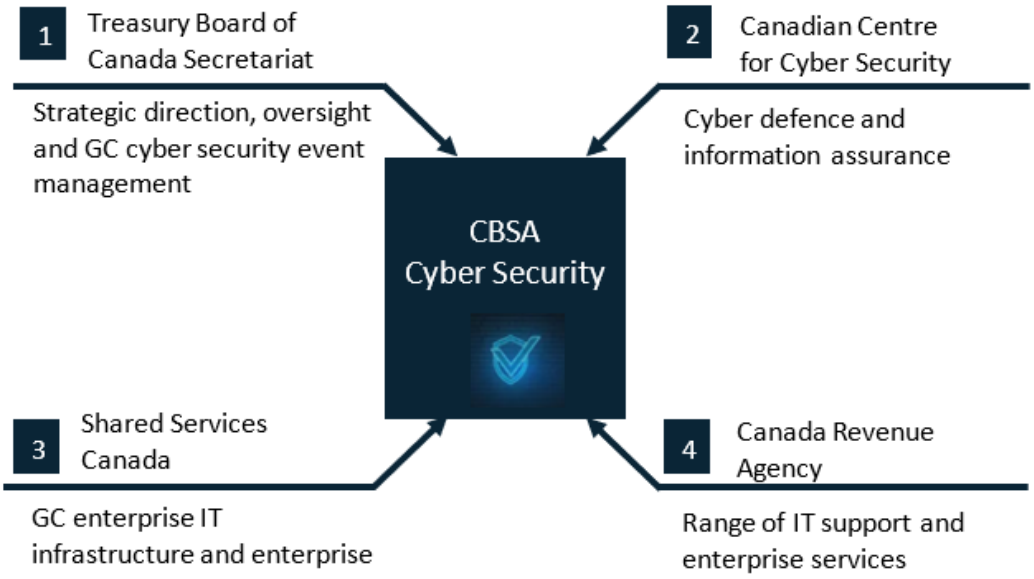
With the CSO function (SPSD) newly reporting to the VP of RSPIB, there is an opportunity to revisit and reaffirm this agreement to ensure continued clarity of functional roles and responsibilities.

While the agency's framework and the agreement between senior officials clarified key departmental cyber security accountabilities at the organizational level, opportunities remain for the CSD to play a more enabling role in supporting security controls under the PGS and contributing to the establishment of a more integrated and effective security posture for the agency.

External stakeholders

The agency relies on several key external partners to help manage its cyber security program, including SSC, CRA and the Canadian Centre for Cyber Security (the Cyber Centre). Clarity of roles and responsibilities between these parties is essential to support accountability, structure and coordination, particularly given the complexities of a cyber security program and potentially severe impact in case of failure.

Figure 1: Key external stakeholders



- The agency maintained various formal written business agreements with the CRA and SSC, some of which had reached the end of their terms. For example, two service level agreements with the CRA had expired in December 2023; however, they are still being followed while consultations are underway to renew them.
- CSD staff were not fully aware of the CRA and SSC roles and responsibilities, particularly those of the SSC. While they understood their overall mandates and accountabilities, there was limited

awareness related to operational details (refer to the section on Monitoring and oversight for more details). This was due, in part, to gaps and lack of clarity in certain aspects of the memorandums of understanding and service level agreements in place between the agency and these external partners.

Departments and agencies are accountable for managing cyber security risks in their program areas; however, as the whole-of-government adopts an enterprise approach to cyber security and as programs and services become more integrated, it will be imperative that cyber security risks be effectively and holistically managed at the enterprise level in accordance with accountabilities outlined under the Treasury Board policy instruments. Source: *Government of Canada Enterprise Cyber Security Strategy*.

Monitoring and oversight

The newly established Cyber Security Program Management Division in the CSD is responsible for the development, maintenance and progression of the agency's cyber security strategy and its related policies, while ensuring alignment with the priorities and direction of the GC. Its Planning and Reporting Unit is responsible for tracking and reporting on cyber security program delivery, costs, performance and health. However, as the unit was not fully staffed at the time of the audit, its monitoring and oversight activities were limited and focused primarily on enterprise-level risk management activities (refer to the section on Risk Management for more details).

Treasury Board Security Policy Implementation Notice

The 2024 Treasury Board Security Policy Implementation Notice (SPIN) outlines government-wide expectations for improving cyber security posture through standardized security controls, comprehensive protection and proactive management of cyber threats. It also includes specific timelines for federal departments to complete various cyber security activities.

- [redacted]

Monitoring external cyber security support functions

There was no formal mechanism in place within the CSD to validate that other government department partners were fulfilling their cyber/IT security-related responsibilities as intended. The following examples illustrate two important areas where this lack of oversight was observed:

[redacted]

Risk management

Effective cyber security risk management involves identifying, monitoring and managing risks at both operational and strategic levels. In line with GC guidance, these activities help inform decision-making and support departmental security planning.

[redacted]

[redacted]

[redacted]

Cyber maturity self-assessment

The CMSA is a Treasury Board Secretariat developed tool designed to help departments evaluate their cyber security posture against the National Institute of Standards and Technology Cyber Security Framework. The agency has used this tool for four years to assess its maturity across the following five functions: Identify, Protect, Detect, Respond, and Recover.

[redacted]

Table 1: [redacted]

[redacted]

Governance committees and senior management engagement

The Security Program Functional Management Board oversaw the agency's security program (including cyber security) until March 2025. In parallel, the CSD provided ad hoc updates to other agency senior management committees regarding the organisation's cyber security posture and operational challenges. [redacted]

In March 2025, the Security Program Functional Management Board was indefinitely suspended. Subsequently, any requirements for governance committee review of security program-related matters were to be submitted to the Director General Steering Committee. To promote more effective oversight, incorporating more detailed discussions about cyber security risk management into this committee's deliberations would further improve the alignment between the agency's cyber security program objectives and its broader organizational objectives and priorities.

Cyber security event management

The agency is expected to have implemented cyber security event management plans, procedures and processes aligned with GC CSEMP. In line with the GC's Enterprise Cyber Security Strategy and relevant Treasury Board Secretariat policy instruments (including the PGS and related supporting policies, directives and guidelines), these measures would enable timely detection, coordinated response and effective recovery from cyber security events.

The agency is also expected to conduct regular tabletop exercises to validate its response capabilities, with documented results used to identify areas for improvements and enhance organizational resilience.

[redacted]

[redacted]

Recommendation 2

[redacted]

Management response: ISTB agrees with the recommendation and is currently working on strengthening the plans and procedures for detecting and responding to cyber security vulnerabilities and events.

[redacted]

Completion date: April 2026

Government of Canada Cyber Security Event Management Plan

The GC CSEMP establishes a coordinated approach for preventing, detecting, responding to, and recovering from cyber security events across departments. It defines roles, responsibilities and procedures to promote and support consistency in event management practices.

The GC CSEMP defines a cyber security event as any event, act, omission or situation that may be detrimental to government security, including threats, vulnerabilities and incidents. Events may include:

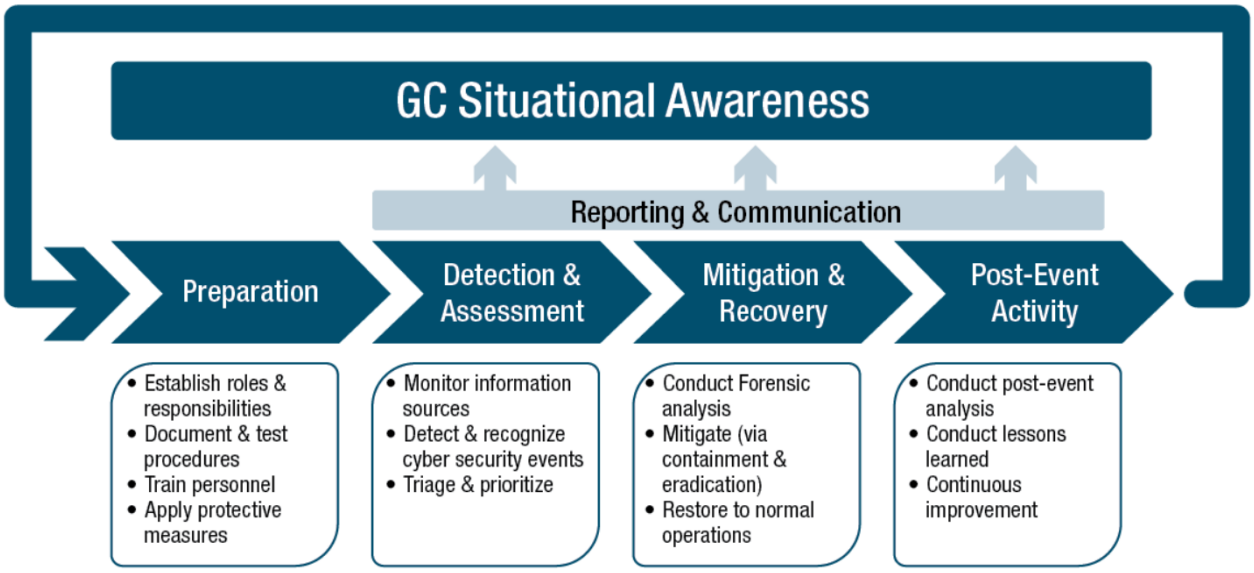
- **Incident:** Any event (or collection of events), act, omission or situation that has resulted in a compromise.
- **Threat:** An activity intended to compromise the security of an information system by altering the confidentiality, integrity, or availability of a system or the information it contains.
- **Vulnerability:** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Cyber security event management process

The CBSA's CSEMP is led primarily by three teams: Incident Response, Advanced Cyber Defence Centre, and Endpoint Protection and Incident Centre. At the agency level, other units support this process, including the Vulnerability Assessment (VA) team and High Availability Response Team. External stakeholders such as CRA, SSC, and the Cyber Centre also play a key role in supporting this process.

[redacted]

Figure 2: Government of Canada Cyber security event management process



A sample of 30 cyber security events was reviewed to assess the agency's compliance with the GC CSEMP and the overall effectiveness and efficiency of its cyber security event management process[1]. The audit examined each event from two perspectives:

- Technical response and containment activities – including identifying, analyzing and addressing the events (detection and mitigation).
- Event coordination and governance activities – such as documenting, reporting, communications, post-event and closeout activities.

Through this dual-lens assessment, the audit examined both the effectiveness and efficiency of core response activities, as well as the adequacy of supporting event coordination and governance activities, in alignment with GC CSEMP requirements (refer to Appendix B for sampling methodology and testing results).

Cyber security event management process testing results

The audit found that technical processes for detecting, assessing, mitigating and recovering from cyber security events were generally effective in supporting the core technical aspects of cyber security event management. [redacted]

[redacted]

[redacted]

[1] Refer to Appendix B, Sampling methodology, for more details

[redacted]

[redacted]

Vulnerability management and security patching

A structured vulnerability and patch management process should be in place to ensure timely assessment, prioritization, deployment and verification of security updates, based on asset criticality and risk exposure. Per the GC CSEMP, robust vulnerability and patch management is essential to mitigating and managing cyber security events. As part of the audit, the agency's vulnerability management practices were assessed by examining 30 national and local/regional applications.

The agency's vulnerability management practices and the CSD's visibility into application security status were assessed through documentation reviews, stakeholder interviews, process walkthroughs and testing of some the agency's applications.

[redacted][2]

Cyber security awareness and training

Cyber security awareness and training activities are important for ensuring all CBSA personnel understand their roles and responsibilities in protecting information and systems. The Treasury Board Directive on Security Management sets out requirements for providing security training and promoting awareness to support secure operations.

At the agency level, the Policy on Security Awareness and Training assigns the DOCS the responsibility for identifying, developing and implementing cybersecurity awareness and training initiatives, in collaboration with the Chief Security Officer's team within SPSD. This includes defining target audiences and developing relevant training products.

Overall finding on cyber security awareness and training

The agency had implemented a cyber security awareness and training strategy; however, activities were not tailored to specific roles or operational needs, and mechanisms to evaluate their effectiveness were limited. These factors hindered the agency's ability to assess the impact, sufficiency and relevance of its awareness and training efforts in relation to its objectives.

Recommendation 3

The VP of ISTB, in collaboration with the VP of RSPIB, should further develop the agency's cyber security awareness program by:

[2] Refer to Appendix B, Sampling methodology for more details.

a) Enhancing the current program to progressively incorporate role-based and targeted awareness initiatives, and ensuring that related learning activities and products are delivered on a more regular basis throughout the year; and
b) Establishing mechanisms to regularly assess the effectiveness of awareness and learning initiatives, including the use of performance measures or evaluation tools to support continuous improvement.

Management response: ISTB agrees with the recommendation. CSD is actively collaborating with CBSA partners to enhance cyber security awareness activities. The goal is to progressively customize the training for various roles and responsibilities and deliver it more regularly throughout the year. The branch is also developing a process to closely monitor the training program's effectiveness, ensuring it can be adapted as needed to meet the evolving demands of the cyber security landscape. Work is progressing on ensuring a successful Cyber Security Awareness Month campaign in October 2025 as well as further integration with the awareness and training efforts on the CBSA Security Program within RSPIB.

The lack of clarity around roles and responsibilities in the CBSA's cyber security program have contributed to the training not yet being tailored as per the demands of the Cyber Security Program. CSD is working on updating the Training and Awareness Strategy in order to augment the effectiveness of awareness and learning initiatives.

Completion date: September 2027

Strategy and plans

Cybersecurity training is crucial for all levels of an organization, from general awareness for all employees to specialized training for those with specific roles and responsibilities and associated risks. The CSD has endorsed a three-year cyber security awareness and training strategy (2024 to 2027) which aims to increase general employee awareness and foster effective cyber security practices, aligning training with evolving threats to strengthen the agency's resilience. This includes collaboration with the SPSD to integrate cyber security into the broader security program initiatives, such as integrating cyber security-related content in the CBSA's Security Awareness week communications. Based on this strategy, the CSD had developed yearly cyber security awareness and training activity plans.

The CSD's cyber security awareness and training strategy recognized the value of providing tailored training and awareness activities and products, and the awareness activities delivered during the audit period covered a variety of topics. However, employee participation was on a voluntary basis, and content was geared towards general awareness. There were no tailored learning or awareness activities or products targeted to specific audiences with different roles or security needs.

A variety of cyber security awareness products were delivered throughout the year and the majority could be accessed through the agency's intranet. Most of these activities and products were delivered annually during the Cyber Security Awareness Month. While these concentrated efforts help raise visibility, delivering awareness content in smaller, recurring modules throughout the year can promote more consistent engagement and support employees in practicing effective cyber security hygiene on an ongoing basis.

- The CSD had prepared an AAR for the October 2024 Cyber Security Awareness Month campaign. According to the AAR, 10 CBSA Daily messages related to Cyber Security Awareness Month were

published; one Atlas Asks was posted on the CBSA intranet; and three presentations were delivered to CBSA employees. Participation across these sessions was limited, with combined attendance estimated at less than 300 individuals (representing less than 2% of the agency's employees).

Training of the cyber security directorate employees

The CSD did not have role-specific training plans for its technical personnel; however, they participated in externally provided courses and received on-the-job training. Although no formal plans with defined timelines were developed, there was recognition of the need for a more structured and formal cyber security training program, particularly for new employees.

Mandatory training for all employees

To enhance employees' cyber security knowledge, the agency provided access to various training courses. Among them, "Insider Threat" and "Discover Cyber Security" were mandatory for all employees, whereas "Recognizing Phishing" was offered as an optional resource.

Similar to all agency's mandatory training courses, tracking the completion of these courses was the responsibility of cost centre managers, who were responsible for following up with their employees as necessary to ensure compliance.

Strengthening collaboration between the CSD and SPSD (for example, leveraging SPSD's operational footprint, subject-matter expertise and regional presence) could support the development of a more unified and risk-informed awareness and training program, better tailored to operational realities and employee needs across the agency. Enhancing this existing collaboration could also contribute to a more strategic use of resources, aligning with agency-wide efforts to improve efficiency and support fiscal responsibility.

Performance measurement

Recognizing security awareness and training as a key control in PGS, the Directive on Security Management mandates ongoing performance measurement and corrective actions to foster continuous improvements in departmental security programs.

Given the value of measurable and behaviour-based performance assessment activities, phishing simulation campaigns are considered effective methods for assessing employee cyber security awareness and the agency's cyber security posture against online threats. As the agency had limited overall performance measurement activities in place, the audit reviewed the extent and frequency of phishing simulations as a key indicator.

- [redacted]

Limited evaluation and assessment activities or processes, such as phishing simulation campaigns, represented a gap in the agency's ability to evaluate the effectiveness of its cyber security awareness and training efforts. Without regular and structured evaluation mechanisms, it was difficult for the agency to determine whether its awareness and training objectives were being met or whether its strategies, plans and initiatives needed to be adjusted to reflect organizational needs and evolving cyber security risks.

The effectiveness of the agency's secure operations depends, in part, on the level of cyber security awareness among employees through a well integrated training program. The absence of such a program can limit their ability to recognize and appropriately respond to cyber threats, increasing the risk of operational disruptions. Gaps in awareness can also increase the risk of insider threats – whether through negligence or malicious actions – by limiting employees' understanding of secure behaviours and organizational expectations. Weaknesses in one organization's security awareness can also be exploited by threat actors to gain unauthorized access or to launch broader attacks across interconnected departments and systems.

Appendix A: Audit criteria

Lines of enquiry	Audit criteria
1. Governance and risk management	1.1 Departmental cyber security roles and responsibilities are well established and functioning effectively. 1.2 Comprehensive cyber security plans are in place with adequate reporting andmonitoring to address cyber security risks.
2. Controls	2.1 The agency has an effective cyber security event management process in place to prepare and respond to events and incidents in a timely manner. 2.2 A culture of security awareness is supported by tailored awareness and training.

Appendix B: Sampling methodology

The following is an overview of the sampling methodology.

Cyber security event management process testing

What was examined: The audit assessed whether the agency's cyber security event management process aligned with the CBSA/GC CSEMP. A sample of 30 cyber security events were selected and examined. These events occurred between April 01, 2023 , and June 30, 2024.

Data Source: The sample was selected from event tracking logs provided by the CSD. These logs included metadata such as timelines, locations, completion status, impact level and assessment results.

Population and Sampling Approach: The audit applied a judgemental risk-based sampling approach to divide the population to sub-groups based on key risk factors such as event type, status, priority, component (for example, alerts, advisories, phishing/spams). In selecting the final sample, the audit also considered the overall coverage to ensure representation from different sub-groups, where possible.

From the refined population, 30 events were randomly selected across three teams within the Cyber Operations Division:

- Incident Response team: 20 samples
- Endpoint Protection and Event Centre team: 5 samples
- Advanced Cyber Defence Centre: 5 samples

Vulnerability testing

What was examined: The audit reviewed the agency's vulnerability and security patch management practices for its applications to assess how they support different phases of the cyber security event management lifecycle. A total of 30 applications were examined over the period of April 1, 2023, to June 30, 2024.

Data Source: The sample was selected using data obtained from the Application Portfolio Management and Agency Collaboration Platform, in coordination with the Architecture Division, ISTB.

Population and Sampling Approach: The audit selected a sample of national and regional/local applications using a judgemental risk-based approach (for example, prioritizing applications with higher business value and criticality), while aiming to ensure appropriate coverage across different branches and regions where feasible.

The audit selected a total of 30 applications, including:

- CBSA National Applications: 20 samples were selected from the agency's 2023 Application Portfolio Management data
- CBSA Regional/Local Applications: 10 samples were selected from the most recent dataset available in the Agency Collaboration Platform

Appendix C: Acronyms

AAR	After Action Report
CBSA	Canada Border Services Agency
CMSA	Cyber Maturity Self-Assessment
CRA	Canada Revenue Agency
CSD	Cyber Security Directorate
CSEMP	Cyber Security Event Management Plan
CSO	Chief Security Officer
DOCS	Designated Official for Cyber Security
GC	Government of Canada
IR	Incident Response
ISTB	Information, Science and Technology Branch
IT	Information Technology
PGS	Policy on Government Security
RSPIB	Recourse, Standards and Program Integrity Branch
SPIN	Security Policy Implementation Notice
SPSD	Security and Professional Standards Directorate
SSC	Shared Services Canada
VA	Vulnerability Assessment
VP	Vice-President