Audit of Cyber Security at HC and PHAC

Final Report

December 2023

Health Canada and the Public
Health Agency of Canada

Santé Canada et l'Agence
de la santé publique du Canada

Office of Audit and Evaluation

Health Canada is the federal department responsible for helping the people of Canada maintain and improve their health. Health Canada is committed to improving the lives of all of Canada's people and to making this country's population among the healthiest in the world as measured by longevity, lifestyle and effective use of the public health care system.

TO PROMOTE AND PROTECT THE HEALTH OF CANADIANS THROUGH LEADERSHIP, PARTNERSHIP, INNOVATION AND ACTION IN PUBLIC HEALTH.
—Public Health Agency of Canada

Également disponible en français sous le titre :
Audit de la cybersécurité à Santé Canada et à l'ASPC

To obtain additional information, please contact:

Health Canada / Public Health Agency of Canada
Address Locator 0900C2
Ottawa, ON K1A 0K9
Tel.: 613-957-2991
Toll free: 1-866-225-0709
Fax: 613-941-5366
TTY: 1-800-465-7735
E-mail: publications-publications@hc-sc.gc.ca

Publication date: December 2023

Cat.: H14-594/2024E-PDF
ISBN: 978-0-660-71104-1
Pub.: 240022

Table of Contents

Executive Summary

Introduction

Since the onset of the COVID-19 pandemic, network connectivity continues to increase at an exponential rate. This places businesses and governments at an increased risk of cyber attacks, which are becoming more frequent and sophisticated. Therefore, cyber security has become an area of particular concern and increased importance across all federal government departments.

Cyber security is a whole-of-government responsibility that is shared between Shared Services Canada (SSC), the Communications Security Establishment (CSE), and all other departments and agencies. Health Canada (HC) and the Public Health Agency of Canada (PHAC) rely on SSC for its Enterprise Network and associated infrastructure. SSC acts as a first line of defense for cyber security by continuously monitoring Government of Canada networks and servers, and providing perimeter protection. Additionally, the CSE, specifically the Canadian Centre for Cyber Security (CCCS), provides government-wide cyber security monitoring and issues alerts and guidance to departments. HC and PHAC are responsible for all end-point activities, including desktop monitoring, business application logs, and awareness campaigns on issues such as phishing and user activities.

Cyber security is a shared responsibility within HC and PHAC. Since its creation in April 2022, the Digital Transformation Branch (DTB) has split responsibility for cyber security with the Corporate Services Branch (CSB). As per the Treasury Board of Canada Secretariat's (TBS) *Policy on Government Security* (PGS), the Chief Security Officer (CSO), who is also the Assistant Deputy Minister of CSB, is responsible for the overall creation, governance, and maintenance of security programs. As per the TBS Directive on Service and Digital (DSD), the Designated Official for Cyber Security (DOCS), who is part of DTB, is responsible for the day-to-day cyber security operations, including the Security Assessment and Authorization (SA&A) process. While the ultimate accountability for security, both physical and cyber, rests with the CSO, both branches must work closely together to ensure continued success.

Given the importance of cyber security, and the recent division of responsibilities between DTB and CSB, it is vital to assess whether the current risk management processes and governance structures are working appropriately to allow HC and PHAC to effectively protect themselves from, identify, detect, respond to, and recover from cyber security threats. This audit was suggested as the first of a series of potential assurance engagements on cyber security to ensure that key governance and risk management concepts are in place and operating effectively. Additional projects are being considered as part of Risk-based Audit Plan updates.

Engagement Objective

The objective was to assess the effectiveness of IT security governance and risk management processes designed to counter and mitigate cyber security risks faced by HC and PHAC. Please refer to Appendix B for further details on the audit scope, criteria, methodology, and approach, as well as a statement of conformance.

Overall Conclusions

Overall, HC and PHAC have implemented elements of the governance and risk management processes needed to identify and mitigate cyber security risks. Specifically, HC and PHAC have designated cyber security officials to promote accountability, have implemented a process for managing cyber incidents, and have outlined roles and responsibilities for the IT Security group and other stakeholders via published standards and guidelines. HC and PHAC have also identified and assessed high-level risks in corporate documents, defined processes for conducting risk assessments at an operational level, established agreements with third parties and stakeholders to support IT security activities, and proposed a new intra-departmental IT security committee to senior management as of the end of the audit's conduct phase.

The audit identified the following opportunities to further improve the key governance and risk management processes at HC and PHAC:

- The internal governance structure supporting cyber security activities, including senior management committees, did not regularly discuss cyber security issues to promote awareness and help facilitate decision making. This lack of communication can result in key issues being missed or not being communicated in a timely manner, efforts being duplicated, and can lead to a lack of accountability for the management of cyber security.
- The governance structure has not been recently reviewed for continued relevance, considering the Department's recent restructuring efforts, to ensure roles and responsibilities are adequately reflected. In addition, key documentation does not sufficiently delineate roles and responsibilities between CSB and DTB. A lack of clear roles and responsibilities for cyber security, at a general level and in the context of governing bodies, may lead to an inefficient use of resources, duplication of effort, a lack of accountability, and a lack of the collaboration required to respond to and prevent cyber security threats, particularly in the new DTB-CSB context.
- Cyber security risks identified by HC and PHAC were not formally prioritized, tracked, nor monitored, and HC relied on informal relationships between security partners to communicate information internally and mitigate risks. This could result in cyber security related risks that are not considered or efficiently managed, placing both organizations at greater risk of cyber attacks.
- There was limited tracking and reporting on performance as it relates to managing cyber security, which could lead to ineffective processes for managing and mitigating cyber security risks, thus leading to cyber attacks that could have been prevented.

Context

It is important to have a clearly defined and well understood governance structure, including defined roles and responsibilities related to cyber security, in order to effectively prevent and mitigate cyber threats.

Within HC and PHAC, security activities and responsibilities are divided between DTB's IT Security Team and CSB's National Security Management Division (NSMD).

Activities related to cyber security in DTB are primarily governed by the TBS Directive on Service and Digital. Activities for security in general, including cyber security, are primarily governed by the TBS Directive on Security Management.

What did we expect to find?

We expected to find that the governance structure supporting cyber security would provide effective oversight over key departmental IT security activities, and that it would ensure alignment with applicable policies, directives, and standards. Moreover, we expected to find that roles and responsibilities were clearly defined, that security officials were appropriately designated, and that committees worked in accordance with their established mandates, and shared key information with decision makers in a timely manner. We expected that agreements were in place with key partners and that the governance structure was reviewed on an ongoing basis to ensure continued relevance and effectiveness.

Findings

Overall, we found that HC and PHAC had designated officials, such as the CIO, CSO, and DOCS, with responsibility and accountability for cyber security. HC and PHAC have documented processes for managing individual cyber incidents, and the roles and responsibilities for operational-level IT security committees were well defined. However, we found that the broader governance structure supporting cyber security, including informal reporting relationships and the expectations of other relevant committees, was not clearly documented. In addition, senior management committees meant to provide strategic direction on cyber security had either not met regularly during the audit period or had not discussed cyber security. This lack of systematic reporting on cyber security during committee meetings could lead to management being unaware or not understanding the volume and nature of cyber security breaches. It could also increase the amount of coordination and oversight needed to effectively manage cyber security risks. In addition, an undocumented governance structure and process could lead to miscommunication and duplication of effort within the Department and Agency.

HC and PHAC have relied on informal reporting relationships to communicate information on cyber incidents, overarching risks, and governance decisions. In addition, there is no formal reporting to senior management within the Department and Agency. As a result, expected committee functions, such as monitoring outstanding risks, reporting changes in the risk environment, and assessing performance have been handled through alternate means, generally on an incident-by-incident basis. For example, cyber security performance was assessed when reporting to senior management on TBS-led initiatives like the Departmental Plan for Service and Digital (DPSD) and the Cyber Maturity Self-Assessment (CMSA), as well as during exercises to ensure alignment with CSE guidance. Informal reporting structures and processes could lead to a breakdown in communication, resulting in key issues being missed or not being communicated to the appropriate people in a timely manner, efforts being duplicated, and lead to a lack of accountability for cyber security related responsibilities.

General roles and responsibilities for cyber security, including the role of the IT Security Team, the CIO, and the Deputy Chief Security Officer (DCSO) in NSMD, were outlined in the 22 approved IT Security Standards and Guidelines available to employees on the intranet, as well as in the HC and PHAC 2019 to 2022 Departmental Security Plans (DSP). The Shared Services Partnership Agreement also outlined roles, responsibilities, and accountabilities between these groups. Although most (77%) of the IT Security Standards and Guidelines had been reviewed since January 2020, few had been updated since DTB's creation in April 2022 to reflect the recent change of roles and responsibilities in CSB and DTB. As of the end of the audit's conduct phase, the DSPs were also due for updates and had not been reviewed as required by the TBS *Policy on Government Security*. A lack of clear roles and responsibilities for cyber security, at a general level and in the context of governing bodies, may lead to an inefficient use of resources, duplication of effort, and a lack of collaboration required to respond to and prevent cyber security threats, particularly in the new DTB-CSB context.

Lastly, the governance structure has not undergone a broader comprehensive review to ensure its continued relevance and effectiveness, and to ensure committees in place were having discussions on cyber-related items. Regular reviews of cyber security processes were conducted through TBS-mandated initiatives, such as the DPSD and the CMSA, and some components of these reviews, particularly in the CMSA, were related to governance. However, given the recent split of responsibilities for cyber security between CSB and DTB, it would be particularly important to formally review the governance structure in order to ensure effective communication between the CIO, CSO, DOCS, the Information Technology Security Coordinator (ITSC), and their respective teams. This may require work beyond the proposed intra-departmental security committee, especially when it comes to formal reporting relationships. An ineffective governance structure could lead to untimely or uninformed decision-making, key issues not being corrected, siloed activities, and an inefficient use of resources.

It should be noted that, in order to streamline communications and mitigate risks, a new intra-departmental committee on IT security was proposed to senior management during the audit period. However, the committee had not been put in place as of the end of the audit's conduct phase.

Conclusion

Overall, HC and PHAC have put in place elements of a governance framework to establish and maintain an appropriate cyber security posture. However, there were opportunities to improve information sharing, reporting, and monitoring to facilitate decision making at the senior management levels. Discussions on issues such as priorities, trends, concerns, and emerging controls should be held at either senior management levels or at the new intra-departmental committee on IT security. Key governance documents should also be updated to ensure roles and responsibilities between DTB and CSB are clearly defined and understood. Without a clear understanding of roles and responsibilities, cyber security risks might not be managed appropriately, which could increase the risk of cyber attacks at the Department and Agency.

Recommendation 1: It is recommended that the ADM of DTB, who is the Designated Official for Cyber Security, in collaboration with the CIO and the ADM of CSB, who is also the CSO, review, update, document, and communicate the existing cyber security governance structure and committees to reflect the new DTB-CSB operating context, and to ensure that senior management is kept informed of potential and evolving cyber security issues, risk management practices, and performance metrics. These, in turn, will enable them to make informed decisions and provide strategic direction on how to mitigate anticipated cyber security related issues.

Criterion 2 – Risk Management

Context

The Directive on Security Management (DSM) and the Policy on Service and Digital (PSD) both provide guidance on expected cyber security risk management activities. Additionally, existing standard operating procedures outline how risks should be identified, assessed, monitored, and reported.

While SSC and CCCS are responsible for providing government wide cyber threat monitoring, HC and PHAC are responsible for monitoring all end-point activities, as well as assessing, prioritizing, and mitigating identified risks, as needed.

What did we expect to find?

We expected to find that risk management processes were in place and followed to identify, assess, and prioritize cyber security risks. We expected that these processes would be well documented and aligned with relevant government policies, directives, and best practices. Additionally, we expected that risk management processes would include the identification of appropriate risk mitigation strategies and recommendations to senior management on how to improve HC and PHAC's overall cyber security posture.

Findings

Overall, we found that HC and PHAC had defined risk management processes for identifying and assessing cyber related risks, but only at the operational and cyber incident specific levels. These processes were documented in internal standard operating procedures, and other supporting documentation. We also found that risks were being tracked at an enterprise level via the DSPs and the Corporate Risk Profile (CRP). However, we found the processes to prioritize and track risks across HC and PHAC to be insufficient, particularly as there was no centralized cyber security risk register. Additionally, monitoring and reporting on cyber threats was conducted informally, on an as needed basis, and heavily focused on incident-specific reporting.

Operational risk management processes were well documented, particularly those relating to the Security Assessment and Authorization (SA&A) process. However, the documentation was not regularly reviewed, nor updated for continued accuracy, with some sections being out of date. For example, as noted above, most of the standards available on the intranet had not been updated to capture the recent change in responsibilities in DTB and CSB, leaving the sections on accountability out of date. If risk management processes are not updated regularly, planning processes may not reflect the current risk landscape and risks could be overlooked, putting the Department and Agency at a greater risk of cyber attacks.

There was no centralized risk register in place to monitor trends in the risk landscape and ensure risks were not overlooked. Business application risks were assessed formally through the SA&A process, but information to track or prioritize risks was not formally captured between assessments. Although the enterprise-level risks were considered in the DSPs and the CRP, the prioritization of cyber security risks was primarily discussed through informal e-mails and discussions, which could lead to some risks being overlooked and unassessed, thus making current controls less effective and ultimately increasing the risk of successful cyber attacks.

While published standards and guidelines outline monitoring and reporting requirements for cyber risk management activities, data on these metrics has not been consistently collected or reported in a formal manner. Most of the reporting to senior management was based on cyber security incidents as they occurred. All examples of reports provided to the audit team on the risk landscape and mitigating controls were less than a year old, with no reports provided between January 2020 and January 2022. The IT incident reports did not include information to track performance over time, making it difficult to identify risk management performance trends. As of the end of the audit's conduct phase, informal reporting mechanisms, such as emails, calls, and scheduled bilateral meetings, were the primary method by which reports and information related to cyber security were shared with senior management, including the CIO, DOCS, and DCSO. Informal reporting structures could lead to miscommunication, as well as key issues being missed or not being communicated to the appropriate people in a timely manner, efforts being duplicated, and lead to a lack of accountability.

It is important to note that TBS-mandated reporting activities, such as the CMSA, were being leveraged to report to senior management on current risk management processes, inform risk assessments, identify opportunities for improvement, and plan next steps. However, this was not done in a regular nor scheduled manner, nor as part of a formal governance framework. Recommendation 1 includes the requirement to implement formal reporting processes to ensure stakeholders are kept informed on current and planned initiatives; regular reporting on present, potential, and evolving cyber security issues; effective risk management in the new DTB-CSB context; and performance metrics. Having this in place will help senior management make informed decisions and provide strategic direction on how to mitigate anticipated cyber security related issues.

Conclusion

Overall, HC and PHAC have implemented some risk management processes to identify, assess, and prioritize cyber security risks at HC and PHAC. However, there were opportunities to improve risk prioritization and tracking across both organizations. In addition, HC and PHAC should ensure that their standards reflect the updated roles and responsibilities of DTB and CSB, and that monitoring and reporting on the effectiveness of cyber security risk management is done in a more formal manner. If cyber risks are not prioritized and monitored, this could lead to an ineffective cyber security posture and cause disruptions in operations at both HC and PHAC in the event of a successful cyber attack.

Recommendations
Recommendation 2: It is recommended that the ADM of DTB, in collaboration with the CIO and the ADM of CSB, implement a centralized system for tracking and prioritizing cyber security risks by capturing risks from internal processes such as SA&As, trends identified by the Canadian Centre for Cyber Security, and risks from government-wide monitoring.

Appendix A - Scorecard

Audit of Cyber Security at HC and PHAC

Criterion	Risk Rating (residual risk without implementing the recommendation)	Risk Remaining without Implementing Recommendation	Rec #
Criterion 1: HC and PHAC has implemented a governance framework to establish and maintain an appropriate cyber security posture.	3	An inadequate governance framework has negative impacts on all cyber security activities and, as such, frameworks are necessary to provide strategic direction, promote collaboration, and establish appropriate risk management processes. Therefore, a cyber security governance framework that is not functioning as expected may affect the organization's ability to identify, protect, detect, respond to, and recover from cyber events. Furthermore, a lack of formality and consistency in how cyber security is managed means that both HC and PHAC are operating reactively, instead of proactively, which may leave outstanding risks related to business continuity and ensuring information is getting to decision makers in a timely manner to help facilitate decisions. Given that HC and PHAC have proposed implementing an intra-departmental IT security committee, the risk rating for this criterion is moderate. However, given the recent organizational restructuring of security activities between CSB and DTB, HC and PHAC would benefit from reviewing the governance structure to ensure that cyber risks continue to be managed and mitigated as required.	1
Criterion 2: Processes are in place to identify, assess and prioritize IT Security risks, including the identification of appropriate mitigation measures.	2	Effective risk management processes are vital to ensuring that cyber risks faced by both organizations are appropriately identified, assessed, prioritized, mitigated, and reported. As such, if processes are inadequate, risks might not be properly managed or addressed, leaving HC and PHAC vulnerable to cyber attacks. Although risks are managed at strategic and operational levels, they have not been formally prioritized, tracked, nor monitored, and HC and PHAC have relied on informal relationships between security partners to communicate information and mitigate risks.	2

1	2	3	4	5
Minimal Risk	Minor Risk	Moderate Risk	Significant Risk	Major Risk

Appendix B – About the Audit

1. Audit Objective

The objective was to assess the effectiveness of IT security governance and risk management processes designed to counter and mitigate cyber security risks faced by HC and PHAC.

2. Audit Criteria

Criterion 1 – HC and PHAC have implemented a governance framework to establish and maintain an appropriate cyber security posture.
Criterion 2 – Processes are in place to identify, assess, and prioritize IT security risks, including the identification of appropriate mitigation measures.

3. Audit Scope

The scope was limited to IT security governance and risk management processes that HC and PHAC have implemented to mitigate cyber attacks on their information and IT assets. The audit did not examine the adequacy of technical controls to prevent, monitor, detect, respond to, and recover from cyber attacks. These areas may be subject to future audits. The audit also excluded the National Microbiology Laboratory Branch within PHAC, as this is the subject of a separate concurrent audit on cyber security.

4. Audit Approach

The audit approach included, but was not limited to:

- Interviews with senior management and employees; and
- Review of relevant documentation and related controls.

5. Statement of Conformance

This audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing* and is supported by the results of the Office of Audit and Evaluation's Quality Assurance and Improvement Program.