Audit de la cybersécurité à Santé Canada et à l'ASPC

Rapport définitif

Décembre 2023

Santé Canada est le ministère fédéral responsable d'aider les Canadiennes et les Canadiens à maintenir et à améliorer leur état de santé. Santé Canada s'est engagé à améliorer la vie de tous les Canadiens et à faire du Canada l'un des pays où les gens sont le plus en santé au monde, comme en témoignent la longévité, les habitudes de vie et l'utilisation efficace du système public de soins de santé.

PROMOUVOIR ET PROTÉGER LA SANTÉ DES CANADIENS GRÂCE AU LEADERSHIP, AUX PARTENARIATS, À L'INNOVATION ET AUX INTERVENTIONS EN MATIÈRE DE SANTÉ PUBLIQUE.
— Agence de la santé publique du Canada

Also available in English under the title:
Audit of Cyber Security at HC and PHAC

Pour obtenir plus d'information, veuillez communiquer avec :

Santé Canada / Agence de la santé publique du Canada
Indice de l'adresse 0900C2
Ottawa (Ontario) K1A 0K9
Tél. : 613-957-2991
Sans frais : 1-866-225-0709
Téléc. : 613-941-5366
ATS : 1-800-465-7735
Courriel : publications-publications@hc-sc.gc.ca

Date de publication : décembre 2023

Cat. : H14-594/2024F-PDF
ISBN : 978-0-660-71105-8
Pub. : 240023

Table des matières

Introduction

Depuis le début de la pandémie de COVID 19, la connectivité de réseau continue à augmenter à une vitesse exponentielle. Les entreprises et les gouvernements sont donc exposés à un risque accru de cyberattaques, qui deviennent de plus en plus fréquentes et sophistiquées. C'est pourquoi la cybersécurité est devenue un domaine particulièrement préoccupant et de plus en plus important pour tous les organismes du gouvernement fédéral.

La cybersécurité est une responsabilité pangouvernementale partagée entre Services partagés Canada (SPC), le Centre de la sécurité des télécommunications (CST) et tous les autres ministères et agences. Santé Canada (SC) et l'Agence de la santé publique du Canada (ASPC) font appel à SPC pour leur réseau d'entreprise et l'infrastructure connexe. SPC constitue la première ligne de défense en matière de cybersécurité en surveillant les réseaux et les serveurs du gouvernement du Canada de façon continue et en assurant la protection du périmètre. De plus, le CST, plus précisément le Centre canadien pour la cybersécurité (CCC), assure la surveillance de la cybersécurité à l'échelle du gouvernement et émet des alertes et des conseils à l'intention des ministères. Santé Canada et l'ASPC sont responsables de toutes les activités relatives aux points finaux, y compris la surveillance des ordinateurs de bureau, les journaux des applications professionnelles et les campagnes de sensibilisation sur des questions telles que l'hameçonnage et les activités des utilisateurs.

La cybersécurité est une responsabilité partagée au sein de Santé Canada et de l'ASPC. Depuis sa création, en avril 2022, la Direction générale de la transformation numérique (DGTN) partage la responsabilité en matière de cybersécurité avec la Direction générale des services de gestion (DGSG). Conformément à la Politique sur la sécurité du gouvernement (PSG) du Secrétariat du Conseil du Trésor du Canada (SCT), le dirigeant principal de la sécurité (DPS), qui est également le sous ministre adjoint de la DGSG, est chargé de la création, de la gouvernance et de la mise à jour des programmes de sécurité. Conformément à la Directive sur les services et le numérique (DSN) du SCT, l'agent désigné pour la cybersécurité (ADC), qui fait partie de la DGTN, est chargé des opérations quotidiennes de cybersécurité, y compris le processus d'évaluations et d'autorisations de sécurité (EAS). Bien que la responsabilité ultime de la sécurité, tant la sécurité physique que la cybersécurité, incombe au DPS, les deux directions générales doivent travailler en étroite collaboration pour garantir un succès continu.

Étant donné l'importance de la cybersécurité, ainsi que la récente répartition des responsabilités entre la DGTN et la DGSG, il est essentiel d'évaluer si les processus de gestion des risques et les structures de gouvernance actuels fonctionnent correctement pour permettre à Santé Canada et à l'ASPC de se protéger efficacement contre les menaces en matière de cybersécurité, de les reconnaître, de les détecter, d'y réagir et d'y remédier. Cet audit a été proposé comme le premier d'une série de missions d'assurance potentielles en matière de cybersécurité afin de garantir que les concepts clés de gouvernance et de gestion des risques sont en place et fonctionnent efficacement. D'autres projets sont envisagés dans le cadre des mises à jour du Plan d'audit axé sur les risques.

Résumé

Objectif de la mission

L'objectif était d'évaluer l'efficacité des processus de gouvernance et de gestion des risques en matière de sécurité des TI conçus pour contrer et atténuer les risques en matière de cybersécurité auxquels Santé Canada et l'ASPC sont confrontés. Veuillez consulter l'annexe B pour plus de détails sur la portée de l'audit, les critères, la méthodologie et l'approche, ainsi que pour un énoncé de conformité.

Conclusions générales

Globalement, Santé Canada et l'ASPC ont mis en œuvre les éléments des processus de gouvernance et de gestion des risques nécessaires pour reconnaître et atténuer les risques en matière de cybersécurité. Plus précisément, Santé Canada et l'ASPC ont désigné des responsables de la cybersécurité pour promouvoir la responsabilisation, ont mis en œuvre un processus de gestion des cyberincidents et ont défini les rôles et responsabilités du groupe de sécurité des TI et des autres intervenants au moyen de normes et de lignes directrices publiées. Santé Canada et l'ASPC ont également indiqué et évalué les risques de haut niveau dans les documents de l'organisation, défini des processus d'évaluation des risques au niveau opérationnel, conclu des accords avec des tiers et des intervenants pour soutenir les activités de sécurité des TI et proposé à la haute direction un nouveau comité de sécurité des TI intraministériel à la fin de la période de l'audit.

L'audit a relevé la possibilité suivante d'amélioration des principaux processus de gouvernance et de gestion des risques à Santé Canada et à l'ASPC :

- La structure de gouvernance interne soutenant les activités de cybersécurité, y compris les comités de la haute direction, ne discutait pas régulièrement des questions de cybersécurité afin de promouvoir la sensibilisation et de faciliter la prise de décisions. Ce manque de communication peut avoir pour conséquence que des questions essentielles ne sont pas prises en compte ou ne sont pas communiquées en temps utile, que des efforts sont chevauchés et que la responsabilité de la gestion de la cybersécurité n'est pas assumée.
- La structure de gouvernance n'a pas été récemment réexaminée, compte tenu des récents efforts de restructuration du Ministère et de l'Agence, pour s'assurer qu'elle reste pertinente et que les rôles et les responsabilités sont pris en compte de manière adéquate. De plus, la documentation clé ne délimite pas suffisamment les rôles et les responsabilités de la DGSG et de la DGTN. L'absence de rôles et de responsabilités clairs en matière de cybersécurité, au niveau général et dans le contexte des organes directeurs, peut conduire à une utilisation inefficace des ressources, à un chevauchement des efforts, à un manque de responsabilité et à l'absence de la collaboration nécessaire pour réagir aux menaces de cybersécurité et les prévenir, en particulier dans le nouveau contexte DGTN-DGSG.
- Les risques en matière de cybersécurité relevés par Santé Canada et l'ASPC n'ont pas fait l'objet d'une priorisation, d'un suivi ou d'un contrôle formels et Santé Canada s'est appuyé sur des relations informelles entre les partenaires en matière de sécurité pour communiquer des informations à l'interne et atténuer les risques. Il pourrait en résulter des risques en matière de cybersécurité qui ne seraient pas pris en compte ou gérés efficacement, ce qui exposerait les deux organisations à un risque accru de cyberattaques.
- Le suivi et l'établissement de rapports sur le rendement en matière de gestion de la cybersécurité sont limités, ce qui pourrait rendre inefficaces les processus de gestion et d'atténuation des risques en matière de cybersécurité, entraînant ainsi des cyberattaques qui auraient pu être évitées.

Contexte

Il est important de disposer d'une structure de gouvernance clairement définie et bien comprise, incluant des rôles et des responsabilités définis en matière de cybersécurité, afin de prévenir et d'atténuer efficacement les cybermenaces.

Au sein de Santé Canada et de l'ASPC, les activités et les responsabilités en matière de sécurité sont réparties entre l'équipe de sécurité des TI de la DGTN et la Division générale de la sécurité nationale (DGSN) de la DGSG.

Les activités liées à la cybersécurité au sein de la DGTN sont principalement régies par la Directive sur les services et le numérique du SCT. Les activités relatives à la sécurité en général, y compris la cybersécurité, sont principalement régies par la Directive sur la gestion de la sécurité du SCT.

Que nous attendions-nous à trouver?

Nous pensions constater que la structure de gouvernance soutenant la cybersécurité assure une surveillance efficace des principales activités ministérielles de sécurité des TI et qu'elle garantit une harmonisation avec les politiques, les directives et les normes pertinentes. Nous pensions de plus constater que les rôles et responsabilités étaient clairement définis, que les responsables de la sécurité étaient désignés de manière appropriée et que les comités travaillaient conformément aux mandats qui leur ont été confiés, les informations clés étant partagées en temps utile avec les décideurs. Nous nous attendions à ce que des accords aient été conclus avec les principaux partenaires et à ce que la structure de gouvernance soit réexaminée de manière continue afin de garantir sa pertinence et son efficacité.

Constatations

Globalement, nous avons constaté que Santé Canada et l'ASPC ont désigné des responsables, tels que le DPI, le DPS et l'ADC, qui sont chargés de la cybersécurité et qui doivent rendre compte à ce sujet. Santé Canada et l'ASPC disposent de processus documentés pour gérer les différents cyberincidents, et les rôles et responsabilités des comités de sécurité des TI du niveau opérationnel ont été bien définis. Nous avons toutefois constaté que la structure de gouvernance plus large soutenant la cybersécurité, y compris les relations hiérarchiques informelles et les attentes des autres comités concernés, n'était pas clairement documentée. De plus, les comités de la haute direction chargés de donner une orientation stratégique en matière de cybersécurité ne s'étaient pas réunis régulièrement au cours de la période d'audit ou n'avaient pas abordé la question de la cybersécurité. Cette absence de rapports systématiques sur la cybersécurité lors des réunions des comités pourrait faire en sorte que la haute direction ne soit pas avisée du volume et de la nature des atteintes à la cybersécurité ou qu'elle ne comprenne pas bien ces éléments. Elle pourrait également accroître le niveau de coordination et de surveillance nécessaire pour gérer efficacement les risques en matière de cybersécurité. De plus, une structure et un processus de gouvernance non documentés pourraient entraîner une mauvaise communication et un chevauchement des efforts au sein du Ministère et de l'Agence.

Santé Canada et l'ASPC se sont appuyés sur des relations hiérarchiques informelles pour communiquer des informations sur les cyberincidents, les risques globaux et les décisions de gouvernance. De plus, il n'existe pas de lien hiérarchique formel avec la haute direction au sein du Ministère et de l'Agence. En conséquence, les fonctions attendues du comité, telles que le suivi des risques en suspens, la notification des changements touchant le contexte de risque et l'évaluation du rendement, ont été traitées par d'autres moyens, généralement incident par incident. Par exemple, le rendement en matière de cybersécurité a été évalué lors de l'établissement de rapports à l'intention de la haute direction sur des initiatives menées par le SCT, telles que le Plan ministériel sur les services et le numérique (PMSN) et l'auto évaluation de la cybermaturité (AEC), ainsi que lors d'exercices visant à garantir l'harmonisation avec les orientations du CST. Les structures et processus informels de production de rapports pourraient entraîner une rupture de la communication, ce qui aurait pour conséquence que des questions essentielles ne seraient pas abordées ou ne seraient pas communiquées en temps opportun aux personnes concernées, qu'il y aurait un chevauchement des efforts et qu'on entraînera un manque de comptabilité en ce qui concerne les responsabilités en matière de cybersécurité.

Les rôles et responsabilités généraux en matière de cybersécurité, y compris le rôle de l'équipe de sécurité des TI, du DPI et du dirigeant principal adjoint de la sécurité (DPAS) au sein de la DGSN, ont été décrits dans les 22 normes et lignes directrices approuvées en matière de sécurité des TI auxquelles les employés ont accès dans l'intranet, ainsi que dans les plans de sécurité ministériels (PSM) 2019 2022 de Santé Canada et de l'ASPC. L'accord sur les services partagés a également défini les rôles, les responsabilités et les obligations de rendre compte de ces groupes. Bien que la plupart (77 %) des normes et lignes directrices en matière de sécurité des TI aient été révisées depuis janvier 2020, peu d'entre elles ont été mises à jour depuis la création de la DGTN en avril 2022 afin de refléter le récent changement de rôles et de responsabilités au sein de la DGSG et de la DGTN. À la fin de la période de l'audit, les PSM devaient également être mis à jour et n'avaient pas été examinés ainsi que l'exige la Politique sur la sécurité du gouvernement du SCT. L'absence de rôles et de responsabilités clairs en matière de cybersécurité, au niveau général et dans le contexte des organes directeurs, peut entraîner une utilisation inefficace des ressources, un chevauchement des efforts et un manque de collaboration nécessaire pour répondre aux menaces de cybersécurité et les prévenir, en particulier dans le nouveau contexte DGTN DGSG.

Enfin, la structure de gouvernance n'a pas fait l'objet d'un examen approfondi pour s'assurer de sa pertinence et de son efficacité et pour faire en sorte que les comités existants discutent des questions liées à la cybersécurité. Des examens réguliers des processus de cybersécurité ont été menés dans le cadre d'initiatives prescrites par le SCT, telles que le PMSN et l'AEC, et certains éléments de ces examens, en particulier dans le cadre de l'AEC, étaient liés à la gouvernance. Toutefois, compte tenu de la récente répartition des responsabilités en matière de cybersécurité entre la DGSG et la DGTN, il serait particulièrement important de revoir officiellement la structure de gouvernance afin d'assurer une communication efficace entre le DPI, le DPS, l'ADC, le coordonnateur de la sécurité des technologies de l'information (CSTI) et leurs équipes respectives. Cela peut nécessiter des travaux allant au delà du comité de sécurité intraministériel proposé, en particulier en ce qui concerne les relations hiérarchiques formelles. Une structure de gouvernance inefficace peut entraîner des prises de décision inopportunes ou mal éclairées, des problèmes clés non corrigés, des activités cloisonnées et une utilisation inefficace des ressources.

Il convient de noter que, afin de rationaliser les communications et d'atténuer les risques, un nouveau comité intraministériel sur la sécurité des TI a été proposé à la haute direction au cours de la période d'audit. Le comité n'avait toutefois pas été constitué à la fin de la période de l'audit.

Conclusion

Globalement, Santé Canada et l'ASPC ont mis en place les éléments d'un cadre de gouvernance pour établir et maintenir un dispositif de cybersécurité approprié. Il était toutefois possible d'améliorer le partage d'informations, la production de rapports et la surveillance afin de faciliter la prise de décision au niveau de la haute direction. Des discussions sur des questions telles que les priorités, les tendances, les préoccupations et les contrôles émergents devraient avoir lieu soit au niveau de la haute direction, soit au sein du nouveau comité intraministériel sur la sécurité des TI. Les principaux documents de gouvernance devraient également être mis à jour afin de garantir que les rôles et les responsabilités respectifs de la DGTN et de la DGSG sont clairement définis et compris. Sans une compréhension claire des rôles et des responsabilités, les risques en matière de cybersécurité pourraient ne pas être gérés de manière appropriée, ce qui pourrait accroître le risque de cyberattaques contre le Ministère et l'Agence.

Recommandation 1 : Il est recommandé que le SMA de la DGTN, qui est l'agent désigné pour la cybersécurité, en collaboration avec le DPI et le SMA de la DGSG, qui est aussi le DPS, examine, mette à jour, documente et communique la structure de gouvernance et les comités existants en matière de cybersécurité afin de refléter le nouveau contexte opérationnel de la DGTN DGSG et de faire en sorte que la haute direction soit tenue informée des problèmes potentiels et évoluants en matière de cybersécurité, des pratiques de gestion des risques et des mesures de rendement. Cela leur permettra de prendre des décisions éclairées et de donner des orientations stratégiques sur la manière d'atténuer les problèmes anticipés en matière de cybersécurité.

Critère 2 – Gestion des risques

Contexte

La Directive sur la gestion de la sécurité (DGS) et la Politique sur les services et le numérique (PSN) renferment l'une et l'autre des orientations sur les activités prévues de gestion des risques en matière de cybersécurité. De plus, les procédures opérationnelles normalisées existantes décrivent la manière dont les risques doivent être déterminés, évalués, surveillés et signalés.

Bien que SPC et le CCC soient chargés de surveiller les cybermenaces à l'échelle du gouvernement, Santé Canada et l'ASPC sont chargés de surveiller toutes les activités des points finaux et d'évaluer, de prioriser et d'atténuer les risques relevés, selon le besoin.

Que nous attendions-nous à trouver?

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.