Agence des services frontaliers du Canada | Canada Border Services Agency

Canada

Vérification de la cybersécurité

Agence des services frontaliers du Canada

Canada Border Services Agency

Also available in English:
Audit of cyber security

Vérification de la cybersécurité

Direction de la vérification interne et de l'évaluation des programmes
Septembre 2025

Remarque : [caviardé] indique que des renseignements de nature délicate ont été supprimés en vertu de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*.

Table des matières

Introduction

Les Canadiens comptent sur le gouvernement du Canada (GC) pour offrir des programmes et des services qui sont essentiels à leur santé, à leur sûreté, à leur sécurité et à leur bien-être économique. La présence numérique croissante du GC et son recours aux technologies de l'information pour offrir des programmes et des services font en sorte que les ministères et organismes fédéraux constituent des cibles attrayantes pour les auteurs de cybermenaces ou d'attaques. En raison de la nature délicate et confidentielle des renseignements gérés par l'Agence des services frontaliers du Canada (« ASFC » ou « Agence »), ainsi que de leur grande valeur opérationnelle, les événements liés à la cybersécurité peuvent avoir une incidence importante sur les activités de l'Agence, soit par la perturbation des services essentiels ou par l'exposition de renseignements classifiés ou personnels.

La Direction générale des recours, des normes et de l'intégrité des programmes (DGRNIP), en collaboration avec la Direction générale de l'information, des sciences et de la technologie (DGIST), administre le Programme de sécurité de l'ASFC, qui inclut la cybersécurité. Le programme établit la gouvernance, les contrôles, les pratiques et l'assurance nécessaires pour aider l'Agence à respecter ses

obligations en vertu de la Politique sur la sécurité du gouvernement (PSG), et soutient la prestation sécuritaire des programmes, des services et des priorités de l'ASFC et du GC.

En avril 2024, une Direction de la cybersécurité (DCS) a été mise sur pied au sein de la DGIST grâce à une réorientation des fonctions existantes afin de renforcer davantage sa capacité et de faire progresser les priorités de l'Agence en matière de cybersécurité. La création de la DCS a formalisé, intégré et élargi plusieurs fonctions liées à la cybersécurité qui étaient déjà hébergées au sein de la DGIST, ce qui a permis d'offrir une structure plus unifiée pour appuyer l'élaboration, la gestion et la surveillance du programme de cybersécurité de l'Agence.

Les responsabilités clés de la DCS comprennent :

- Opérations de cybersécurité (Réponse aux incidents (RI), surveillance et gestion des vulnérabilités)
- Gestion des risques, évaluation et conformité
- Solution de sécurité (architecture, génie et intégration)
- Gestion du programme de cybersécurité (planification, gouvernance, normes et rapports)
- Continuité des TI (contribuant au plan de continuité des activités de l'Agence)

À propos de la vérification

L'objectif de la vérification était d'évaluer si le programme de cybersécurité de l'ASFC a mis en œuvre un cadre de contrôle de gestion efficace afin d'appuyer ses objectifs et d'atténuer les menaces et les incidents liés à la cybersécurité.

Inclusions dans la portée de la vérification

La vérification portait sur la période comprise entre le 1er avril 2023 et le 31 mars 2025. Pour cette période, la portée des travaux de vérification ont compris l'examen de la gouvernance, de la gestion des risques et des contrôles en matière de cybersécurité, en portant une attention particulière aux éléments suivants :

- les rôles et responsabilités ministériels au sein de l'Agence;
- les plans visant à gérer les risques liés à la cybersécurité;
- les processus de gestion des événements;
- la sensibilisation et la formation.

Exclusions de la portée de la vérification

La vérification ne portait pas sur les éléments suivants :

- gestion de l'information (y compris l'échange de renseignements avec des tiers);
- activités liées à la cybersécurité menées par des tiers (par exemple, L'Agence du revenu du Canada (ARC) et Services partagés Canada (SPC);
- gestion de la configuration et contrôle des changements;
- sécurité matérielle du matériel de TI.

Note : Au cours de la vérification, la Stratégie intégrée de cybersécurité du GC a été publiée, y compris un modèle opérationnel cible. Par conséquent, l'alignement sur cette approche pangouvernementale était en cours et n'a pas pu être évalué.

Méthodologie de la vérification

- 240 + documents justificatifs examinés
- 60 + parties prenantes consultées
- 11 procédures pas-à-pas réalisées avec les parties prenantes ayant un rôle clé dans les activités de RI de cybersécurité
- 2 tests effectués sur les processus liés à la gestion des événements de cybersécurité, y compris la gestion des vulnérabilités et des correctifs de sécurité

Importance de la vérification

Un programme de cybersécurité efficace repose sur une gouvernance solide et des pratiques de gestion bien définies pour prévenir et détecter les vulnérabilités, les menaces et les incidents cybernétiques et y réagir. Les éléments fondamentaux, comme la gestion des risques, la surveillance et la surveillance du rendement, sont essentiels à la mise en place d'un programme de cybersécurité qui appuie la résilience opérationnelle de l'Agence et renforce sa posture globale en matière de sécurité. Sans eux, l'Agence risque davantage d'être exposée à des perturbations, à des atteintes aux données et à des réponses inappropriées aux menaces qui pourraient compromettre son infrastructure numérique et ses fonds de renseignements de nature délicate.

Un environnement de cybermenaces en évolution, la dépendance de l'Agence envers les intervenants externes pour les services de TI essentiels et les récentes réorientations au sein de la DGIST soulignent le besoin accru de compter sur des rôles et des responsabilités bien définis et sur une robuste structure de gouvernance.

La présente vérification a été approuvée dans le cadre du Plan de vérification axé sur les risques 2024 à 2025.

Énoncé de conformité

La mission de vérification est conforme à la *Politique sur l'audit interne* et à la *Directive sur l'audit interne* du Conseil du Trésor ainsi qu'aux *Normes internationales d'audit interne* de l'Institut des auditeurs internes (IAI). Des éléments de preuve suffisants et appropriés ont été recueillis grâce à diverses procédures pour fournir le niveau d'assurance que procure une vérification. La fonction de vérification interne de l'Agence est indépendante, et les vérificateurs internes ont effectué leur travail avec objectivité, conformément aux *Normes internationales d'audit interne* de l'IAI.

Conclusion de la vérification

Un programme de cybersécurité joue un rôle essentiel dans la prestation sécuritaire des programmes et des services. À mesure que le programme évolue, il améliore la capacité de l'organisation à gérer efficacement les risques liés à la cybersécurité et à maintenir la résilience opérationnelle face à l'évolution du contexte de menace.

L'Agence s'est appuyée sur ses fonctions actuelles en matière de cybersécurité en créant une direction spécialisée. Cependant, plusieurs lacunes connues continuent de présenter des risques pour l'efficacité globale du programme. Il est nécessaire d'intensifier les efforts pour répondre à ces préoccupations. Faire progresser le Programme de cybersécurité, par la finalisation et l'application uniforme des stratégies, des plans, des instruments de politique et des procédures; la clarification des rôles et des responsabilités; l'intégration de pratiques de surveillance régulières améliorera la maturité et l'efficacité du Programme.

Étant donné que la cybersécurité est un élément du portefeuille de la sécurité de l'Agence, il est important que les organismes de gouvernance et les fonctions de sécurité collaborent pour gérer les risques de manière coordonnée et globale. Des progrès soutenus et opportuns dans le renforcement des fonctions de gouvernance, de gestion des risques et de contrôle de la cybersécurité, tout en favorisant une meilleure coordination entre les responsabilités liées à la sécurité, seront essentiels pour assurer une posture de cybersécurité plus mature et plus résiliente pour l'Agence.

Résumé des recommandations

1. [caviardé]
2. [caviardé]
3. Améliorer la sensibilisation et la formation au moyen de contenu personnalisé et d'évaluations régulières de l'efficacité pour appuyer l'amélioration continue.

Réponse de la direction

Le vice-président (VP) de la Direction générale de l'information, des sciences et de la technologie (DGIST) accepte les conclusions de l'audit de la cybersécurité, a reconnu et accepté les recommandations présentées et comprend l'importance de renforcer la position de l'Agence en matière de cybersécurité afin de protéger la confidentialité, l'intégrité et la disponibilité de ses renseignements et de ses biens informatiques. La DGIST participe activement aux efforts visant à mettre en œuvre ces recommandations, en travaillant à la fois de façon indépendante et en collaboration avec d'autres parties concernées de l'Agence et des intervenants externes. [caviardé]. Les résultats de cet audit et de l'AMC orienteront mieux la stratégie pluriannuelle à laquelle la DCS travaille pour améliorer la position de l'ASFC en matière de cybersécurité. L'objectif d'achèvement des activités tient compte de ce qui peut être réalisé en fonction de l'effectif actuel des talents. Si des modifications étaient apportées à la capacité de la main-d'œuvre, l'achèvement pourrait être accéléré.

Constatations de la vérification

La vérification a donné lieux aux résultats suivantes.

Gouvernance et gestion des risques de cybersécurité

Il est attendu que l'Agence ait une approche structurée et intégrée en matière de cybersécurité. Cela comprend la définition, la documentation, la mise en œuvre et le maintien de contrôles de sécurité appropriés, ainsi que l'élaboration d'instruments de politique pour appuyer les interventions opportunes et coordonnées aux événements de cybersécurité. Une approche solide en matière de cybersécurité exige également un cadre de gestion des risques qui intègre la surveillance proactive des menaces et appuie la prise de décisions pour veiller à ce que les risques opérationnels soient surveillés efficacement et utilisés pour orienter la planification de la sécurité ministérielle.

Ces attentes sont fondées sur les principaux instruments de politique du GC qui décrivent les exigences en matière de sécurité ministérielle, de prestation de services numériques et de gestion des événements cybernétiques, dont la Politique sur la sécurité du gouvernement, la Directive sur la gestion de la sécurité, la Politique sur le service et le numérique et la Directive connexe ainsi que le Plan de gestion des événements de cybersécurité (PGEC) du GC. La Stratégie intégrée de cybersécurité du GC renforce encore ces attentes en soulignant la nécessité pour les ministères d'adopter une approche fondée sur les risques, d'améliorer la collaboration entre eux, de réduire les redondances et de renforcer la sécurité et la résilience des services gouvernementaux numériques.

[caviardé]

[caviardé]

Recommandation 1

[caviardé]

Réponse de la direction : La DGIST souscrit à la recommandation et à l'importance de renforcer la gouvernance de l'Agence entourant son programme de cybersécurité.

[caviardé]

Date d'achèvement : Septembre 2026

Instruments de politique et stratégie

Sous la direction du dirigeant principal de la sécurité (DPS) de l'ASFC et de l'agent désigné pour la cybersécurité (ADCS), l'Agence a élaboré huit politiques de sécurité et une série de directives et d'orientations conformes aux exigences du Conseil du Trésor en matière de sécurité du gouvernement. Collectivement, ces politiques sont appelées « Volume de sécurité de l'ASFC ». On peut facilement consulter le Volume sur l'intranet de l'Agence, et la majeure partie de son contenu sur la cybersécurité a été mis à jour en 2024 à 2025.

Depuis sa création, la nouvelle DCS a entrepris des efforts pour élaborer des instruments de politique et des stratégies en matière de cybersécurité qui sont nécessaires à ses fonctions clés. Ces initiatives, qui visaient à renforcer la gouvernance, la gestion des risques et les mesures de contrôle, étaient à diverses

étapes d'élaboration au moment de la vérification. Certaines étaient toujours en ébauche, tandis que d'autres avaient été finalisées et approuvées. Par exemple :

[caviardé]

Parties prenantes internes

La cybersécurité est une responsabilité partagée dans l'ensemble de l'Agence. Bien que de nombreuses unités de la DGIST et de l'Agence aient contribué aux activités de cybersécurité, directement ou indirectement, les principaux intervenants internes ayant des responsabilités principales dans ce domaine étaient la DCS, au sein de la DGIST, et la Direction de la sécurité et des normes professionnelles (DSNP) au sein de la DGRNIP. La DCS est dirigée par l'ADCS, qui était principalement responsable de la cybersécurité, tandis que la DSN relevait du DPS, qui était responsable de la sécurité générale de l'ASFC. À ce titre, l'ADCS et le DPS sont interdépendants et nécessitent une coordination pour soutenir la posture globale de l'Agence en matière de sécurité.

[caviardé]

Le Cadre de gestion du programme de sécurité de l'ASFC décrit les responsabilités des principaux intervenants. Une entente a été signée en novembre 2021 pour clarifier les rôles et responsabilités fonctionnels en matière de cybersécurité, comme suit :

- le VP de la DGIST, qui est également le dirigeant principal de l'information de l'Agence, conserve la responsabilité de la TI et de la cybersécurité;
- le Directeur général de la DSNP, qui est également le DPS de l'Agence, est responsable de la sécurité de la gestion de l'information.

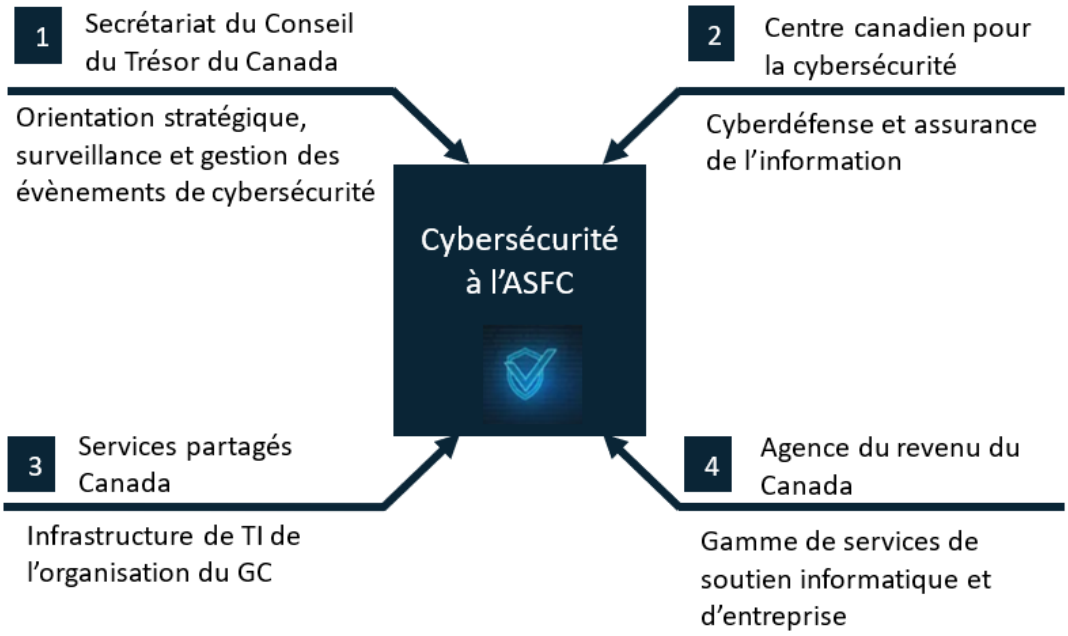
Étant donné que la fonction de DPS (DSNP) relève depuis peu du VP de la DGRNIP, il est possible de réexaminer et de réaffirmer cette entente afin d'assurer la clarté continue des rôles et des responsabilités fonctionnels.

Bien que le cadre de l'Agence et l'entente entre les hauts représentants aient clarifié les principales responsabilités ministérielles en matière de cybersécurité au niveau organisationnel, la DCS a toujours des occasions de continuer de jouer un rôle plus habilitant dans le soutien des contrôles de sécurité en vertu de la PSG et de contribuer à l'établissement d'une posture de sécurité plus intégrée et plus efficace pour l'Agence.

Intervenants externes

L'Agence compte sur plusieurs partenaires externes clés pour aider à gérer son programme de cybersécurité, notamment SPC, l'ARC et le Centre canadien pour la cybersécurité (le Centre pour la cybersécurité). La clarté des rôles et des responsabilités entre ces parties est essentielle pour soutenir la responsabilisation, la structure et la coordination, en particulier compte tenu de la complexité d'un programme de cybersécurité et des répercussions potentiellement graves en cas de défaillance.

Figure 1 : Intervenants externes clés



- L'Agence maintient diverses ententes opérationnelles écrites officielles avec l'ARC et SPC, dont certaines sont venues à échéance. Par exemple, deux ententes sur les niveaux de service avec l'ARC ont expiré en décembre 2023; cependant, elles sont toujours suivies pendant que des consultations sont en cours pour les renouveler.

- Le personnel de la DCS ne connaissait pas pleinement les rôles et les responsabilités de l'ARC et de SPC, en particulier ceux de SPC. Bien qu'ils comprenaient leurs responsabilités et leurs mandats globaux, ils ne connaissaient pas bien les détails opérationnels (se référer à la section sur la Surveillance et contrôle pour plus de détails). Cela s'explique en partie par des lacunes et à un manque de clarté dans certains aspects des protocoles d'entente et des ententes sur les niveaux de service en place entre l'Agence et ces partenaires externes.

Les ministères et organismes sont tenus de gérer les risques liés à la cybersécurité dans leurs secteurs de programme, au fur et à mesure que le gouvernement adopte une approche intégrée en matière de cybersécurité et que les programmes et services deviennent de plus en plus intégrés, il sera essentiel que les risques liés à la cybersécurité soient gérés de façon efficace et globale à l'échelle du GC, selon les responsabilités indiquées dans les instruments politiques du Conseil du Trésor. Source : *Stratégie intégrée de cybersécurité du gouvernement du Canada*.

Surveillance et contrôle

La nouvelle Division de la gestion du programme de cybersécurité (au sein de la DCS) était responsable de l'élaboration, de la mise à jour et de la progression de la stratégie de cybersécurité de l'Agence et de ses politiques connexes, tout en assurant l'harmonisation avec les priorités et l'orientation du GC. Son Unité de planification et de production de rapports est responsable du suivi et de la production de

rapports sur la prestation du programme de cybersécurité, les coûts connexes, ainsi que son rendement et santé. Cependant, comme l'Unité n'était pas entièrement dotée au moment de la vérification, ses activités de suivi et de surveillance étaient limitées et se concentraient principalement sur les activités de gestion des risques à l'échelle de l'organisation (se référer à la section Gestion des risques pour plus de détails).

Avis de mise en œuvre de la Politique sur la sécurité du Conseil du Trésor

L'Avis de mise en œuvre de la Politique sur la sécurité (AMOPS) du Conseil du Trésor de 2024 décrit les attentes à l'échelle du gouvernement pour améliorer la posture en matière de cybersécurité grâce à des contrôles de sécurité normalisés, à une protection complète et à une gestion proactive des cybermenaces. Il précise également combien de temps les ministères fédéraux ont pour mener à bien diverses activités de cybersécurité.

- [caviardé]

Surveiller les fonctions externes de soutien à la cybersécurité

Il n'y avait aucun mécanisme officiel en place au sein de la DCS pour vérifier que les autres ministères partenaires s'acquittaient de leurs responsabilités en matière de sécurité informatique ou de sécurité des TI comme prévu. Les exemples suivants illustrent deux domaines importants où cette absence de surveillance a été observée :

[caviardé]

Gestion des risques

La gestion efficace des risques liés à la cybersécurité comprend l'identification, la surveillance et la gestion des risques aussi bien au niveau opérationnel qu'au niveau stratégique. Conformément aux directives du GC, ces activités aident à éclairer la prise de décisions et soutiennent la planification de la sécurité ministérielle.

[caviardé]

[caviardé]

[caviardé]

Autoévaluation de la maturité cybernétique

L'AMC est un outil élaboré par le Secrétariat du Conseil du Trésor pour aider les ministères à évaluer leur posture en matière de cybersécurité par rapport au Cadre de cybersécurité de l'Institut national des normes et de la technologie. L'Agence utilise cet outil depuis quatre ans pour évaluer sa maturité dans les cinq fonctions suivantes : identifier, protéger, détecter, répondre et récupérer.

[caviardé]

Tableau 1 : [caviardé]

[caviardé]

Comités de gouvernance et mobilisation de la haute direction

Le Conseil de gestion fonctionnelle du programme de sécurité a supervisé le programme de sécurité de l'Agence (y compris la cybersécurité) jusqu'en mars 2025. Parallèlement, la DCS a fourni des mises à jour ponctuelles à d'autres comités de la haute direction de l'Agence concernant la posture de l'organisation en matière de cybersécurité et les défis opérationnels. [caviardé]

Les activités du le Conseil de gestion fonctionnelle du programme de sécurité ont été suspendues pour une période indéterminée en mars 2025. Par la suite, toutes les exigences relatives à l'examen par le comité de gouvernance des questions liées aux programmes de sécurité devaient être soumises au Comité principal des directeurs généraux. Afin de promouvoir une surveillance plus efficace, l'intégration de discussions plus détaillées sur la gestion des risques liés à la cybersécurité dans les délibérations de ce comité améliorerait davantage l'harmonisation entre les objectifs du programme de cybersécurité de l'Agence et ses objectifs et priorités organisationnels plus généraux.

Gestion des événements de cybersécurité

Il est attendu que l'Agence ait mis en œuvre des plans, des procédures et des processus de gestion des événements liés à la cybersécurité, conformément au PGEC GC. Conformément à la Stratégie intégrée de cybersécurité du GC et aux instruments de politique pertinents du Secrétariat du conseil du trésor (y compris la PSG et les politiques, directives et lignes directrices connexes), ces mesures devraient permettre une détection rapide, une intervention coordonnée et une reprise efficace des activités de cybersécurité.

L'Agence doit également effectuer des exercices pratiques réguliers pour valider ses capacités d'intervention, avec des résultats documentés servant à déterminer les points à améliorer ainsi qu'à accroître la résilience organisationnelle.

[caviardé]

[caviardé]

Recommandation 2

[caviardé]

Réponse de la direction : La DGIST souscrit à la recommandation et travaille actuellement à renforcer les plans et les procédures de détection des vulnérabilités et des événements liés à la cybersécurité et les procédures visant à y répondre.

[caviardé]

Date d'achèvement : Avril 2026

Plan de gestion des événements de cybersécurité du gouvernement du Canada

Le PGEC GC établit une approche coordonnée pour prévenir, détecter, répondre et récupérer des événements de cybersécurité dans l'ensemble des ministères. Il définit les rôles, responsabilités et procédures pour favoriser et soutenir la cohérence des pratiques de gestion des événements.

Le PGEC GC définit un événement de cybersécurité comme tout événement, acte, omission ou situation pouvant nuire à la sécurité du gouvernement, y compris les menaces, les vulnérabilités et les incidents. Les événements peuvent inclure :

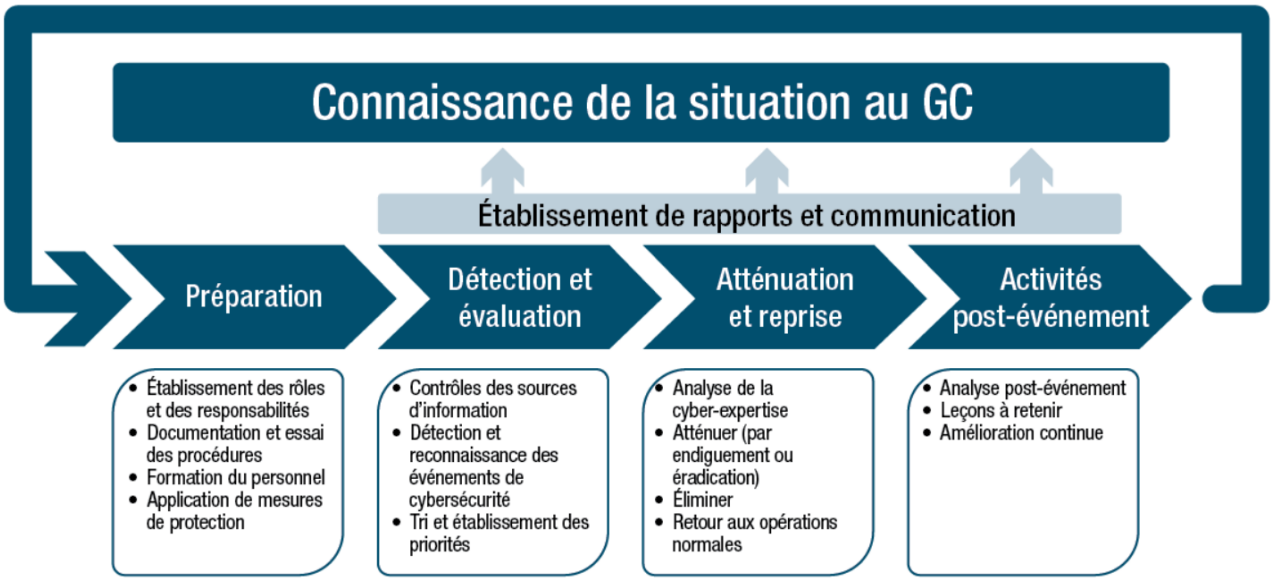
- **Incident :** Tout événement ou série d'événements, acte(s), omission(s) ou toute situation qui a entraîné une compromission.
- **Menace :** Une activité visant à compromettre la sécurité d'un système d'information en altérant la confidentialité, intégrité ou disponibilité du système ou renseignements.
- **Vulnérabilité :** Une faiblesse dans un système d'information, des procédures de sécurité, des mesures de contrôle internes ou la mise en œuvre d'un système qui pourrait être exploitée ou déclenchée par une source de menace.

Processus de gestion des événements de cybersécurité

Le Processus de gestion des événements de cybersécurité de l'ASFC est dirigé principalement par trois équipes : l'équipe d'intervention en cas d'incident, le Centre de cyberdéfense avancé et le Centre de protection des points d'extrémité et d'intervention. Au niveau de l'Agence, d'autres unités ont appuyé ce processus, y compris l'équipe d'évaluation des vulnérabilités (EV) et l'Équipe d'intervention à disponibilité élevée. Des intervenants externes comme l'ARC, SPC et le Centre canadien pour la cybersécurité ont également joué un rôle clé pour soutenir ce processus.

[caviardé]

Figure 2 : Processus de gestion des événements de cybersécurité du gouvernement du Canada



Un échantillon de 30 événements de cybersécurité a été examiné afin d'évaluer la conformité de l'Agence au PGEC du GC et l'efficacité globale ainsi que l'efficience de son processus de gestion des événements de cybersécurité[1]. La vérification a examiné chaque événement de deux points de vue :

- Activités d'intervention technique et de confinement – y compris détection et analyse des événements, ainsi que l'intervention menée pour y répondre (détection et atténuation).
- Coordination des événements et activités de gouvernance – documentation, production de rapports, communications, activités post-événement et activités de clôture.

Dans le cadre de cette évaluation à double perspective, la vérification a examiné à la fois l'efficacité et l'efficience des activités d'intervention de base ainsi que la pertinence de la coordination des événements et des activités de gouvernance, conformément aux exigences du PGEC GC (se référer à l'annexe B pour la méthodologie et les résultats).

Résultats des tests liés au Plan de gestion des événements de cybersécurité

La vérification a permis de constater que les processus techniques de détection, d'évaluation, d'atténuation et de recouvrement pour les événements liés à la cybersécurité étaient généralement efficaces pour appuyer les aspects techniques fondamentaux de la gestion des événements de cybersécurité. [caviardé]

[caviardé]

[caviardé]

[1] Se référer à l'annexe B, Méthode d'échantillonnage, pour obtenir des précisions.

[caviardé]

[caviardé]

Gestion des vulnérabilités et correctifs de sécurité

Un processus structuré de gestion des vulnérabilités et des correctifs devrait être en place pour assurer le caractère opportun de l'évaluation, de l'établissement des priorités, d'un déploiement et d'une vérification des mises à jour de la sécurité, en fonction du caractère essentiel des actifs et de l'exposition aux risques. Selon le PGEC GC, une robuste gestion des vulnérabilités et des correctifs est essentielle pour atténuer et gérer les événements de cybersécurité. Dans le cadre de la vérification, les pratiques de gestion des vulnérabilités de l'Agence ont été évaluées en examinant 30 applications nationales et locales ou régionales.

Les pratiques de gestion des vulnérabilités de l'Agence et la visibilité de la DCS sur le statut de sécurité des applications ont été évaluées au moyen d'examens de la documentation, d'entrevues avec des intervenants, de revues de processus et de mises à l'essai de certaines des applications de l'Agence.

[caviardé][2]

Sensibilisation et formation en matière de cybersécurité

Les activités de sensibilisation et de formation en matière de cybersécurité sont importantes pour veiller à ce que le personnel de l'ASFC comprenne son rôle et ses responsabilités dans la protection de l'information et des systèmes. La Directive sur la gestion de la sécurité du Secrétariat du Conseil du Trésor énonce les exigences relatives à la prestation de formation en matière de sécurité et à la promotion de la sensibilisation à l'appui des opérations sécuritaires.

Au niveau de l'Agence, la Politique sur la sensibilisation et la formation en matière de sécurité attribue à l'ADCS la responsabilité de déterminer, d'élaborer et de mettre en œuvre des initiatives de sensibilisation et de formation en matière de cybersécurité, en collaboration avec l'équipe du dirigeant principal de la sécurité au sein de la DSNP. Cela comprend la définition des publics cibles et l'élaboration de produits de formation pertinents.

Aperçu des constatations sur la sensibilisation et formation en matière de cybersécurité

L'Agence a mis en œuvre une stratégie de sensibilisation et de formation en matière de cybersécurité; cependant, les activités n'ont pas été adaptées à des rôles ou à des besoins opérationnels précis, et les mécanismes d'évaluation de leur efficacité étaient limités. Ces facteurs ont nuit à la capacité de l'Agence d'évaluer l'incidence, le caractère suffisant et la pertinence de ses efforts en matière de sensibilisation et de formation par rapport à ses objectifs.

[2] Se référer à l'annexe B, Méthode d'échantillonnage pour obtenir des précisions.

Recommandation 3

Le VP de la DGIST, en collaboration avec le/la VP de la DGRNIP, devrait développer davantage le programme de sensibilisation à la cybersécurité de l'Agence :

a) en améliorant le programme actuel pour intégrer progressivement des initiatives de sensibilisation axées sur les rôles et ciblées, et veiller à ce que les activités et les produits d'apprentissage connexes soient offerts de façon plus régulière tout au long de l'année ;
b) en établissant des mécanismes pour régulièrement évaluer l'efficacité des initiatives de sensibilisation et d'apprentissage, y compris l'utilisation de mesures de rendement ou d'outils d'évaluation pour appuyer l'amélioration continue.

Réponse de la direction : La DGIST souscrit à la recommandation. La DCS collabore activement avec les partenaires de l'ASFC afin d'améliorer les activités de sensibilisation à la cybersécurité. L'objectif est de personnaliser progressivement la formation en fonction de divers rôles et responsabilités et de l'offrir plus régulièrement tout au long de l'année. La Direction générale élabore également un processus pour surveiller de près l'efficacité du programme de formation, afin de s'assurer qu'il peut être adapté, au besoin, pour répondre aux exigences changeantes du paysage de la cybersécurité. Le travail progresse pour assurer une campagne réussie du Mois de sensibilisation à la cybersécurité en octobre 2025, ainsi qu'une intégration supplémentaire grâce aux efforts de sensibilisation et de formation sur le Programme de sécurité de l'ASFC au sein de la DGRNIP.

Le manque de clarté concernant les rôles et les responsabilités dans le programme de cybersécurité de l'ASFC a contribué à ce que la formation ne soit pas encore adaptée aux exigences du Programme de cybersécurité. La Direction de la cybersécurité travaille à la mise à jour de la Stratégie de formation et de sensibilisation afin d'accroître l'efficacité des initiatives de sensibilisation et d'apprentissage.

Date d'achèvement : Septembre 2027

Stratégie et plans

La formation sur la cybersécurité est essentielle à tous les niveaux d'une organisation, de la sensibilisation générale pour tous les employés à la formation spécialisée pour ceux qui ont des rôles et des responsabilités spécifiques et qui sont exposés aux risques connexes. La DCS a approuvé une stratégie triennale de sensibilisation et de formation à la cybersécurité (2024 à 2027) qui vise à accroître la sensibilisation générale des employés et à favoriser des pratiques efficaces en matière de cybersécurité, en harmonisant la formation avec les menaces en constante évolution afin de renforcer la résilience de l'Agence. Cela comprend la collaboration avec la DSNP pour intégrer la cybersécurité aux initiatives de programme de sécurité élargies, comme l'intégration du contenu lié à la cybersécurité dans les communications de la Semaine de sensibilisation à la sécurité de l'ASFC. À la lumière de cette stratégie, la DCS a élaboré des plans annuels de sensibilisation à la cybersécurité et d'activités de formation.

La stratégie de sensibilisation et de formation à la cybersécurité de la DCS a reconnu la valeur d'offrir des produits et des activités de formation et de sensibilisation sur mesure, et les activités de sensibilisation menées pendant la période d'audit portaient sur une variété de sujets. Cependant, la participation des employés était volontaire, et le contenu visait la sensibilisation générale. Il n'y avait

pas d'activités d'apprentissage ou de sensibilisation adaptées ou de produits destinés à des publics précis ayant des rôles ou des besoins en matière de sécurité différents.

Une variété de produits de sensibilisation à la cybersécurité ont été offerts tout au long de l'année et la majorité d'entre eux ont pu être consultés sur l'intranet de l'Agence. La plupart de ces activités et produits ont été offerts chaque année au cours du Mois de la sensibilisation à la cybersécurité. Bien que ces efforts concentrés contribuent à accroître la visibilité, la présentation de contenu lié à la sensibilisation dans des modules plus petits et récurrents tout au long de l'année peut favoriser une mobilisation plus constante et aider les employés à adopter des pratiques exemplaires et efficaces en matière de cybersécurité de façon continue.

- La DCS avait préparé un RAA pour la campagne du Mois de sensibilisation à la cybersécurité (MSC) d'octobre 2024. Selon le RAA, 10 messages quotidiens de l'ASFC liés au MSC ont été publiés; une question « Atlas vous demande » a été affichée sur l'intranet de l'ASFC; et trois présentations ont été offertes aux employés de l'ASFC. La participation à ces séances était limitée, et le nombre total de participants est estimé à moins de 300 (ce qui représente moins de 2 % des employés de l'Agence).

Formation des employés de la direction de la cybersécurité

La DCS n'avait pas de plans de formation propres à son personnel technique; cependant, ils ont participé à des cours offerts à l'externe et ont reçu une formation en cours d'emploi. Bien qu'aucun plan officiel avec des échéanciers définis n'ait été élaboré, la nécessité d'un programme de formation en cybersécurité plus structuré et plus formel a été reconnue, en particulier pour les nouveaux employés.

Formation obligatoire pour tous les employés

Afin d'améliorer les connaissances des employés en matière de cybersécurité, l'Agence a donné accès à divers cours de formation. Parmi eux, « Menaces internes » et « Découvrez la cybersécurité » étaient obligatoires pour tous les employés, tandis que « Reconnaître l'hameçonnage » était offert en tant que ressource facultative.

Comme pour toutes les formations obligatoires de l'Agence, le suivi de l'achèvement de ces cours était la responsabilité des gestionnaires de centre de coûts, qui étaient chargés d'assurer le suivi auprès de leurs employés, au besoin, pour assurer la conformité.

Le renforcement de la collaboration entre la DCS et la DSNP (par exemple, la mise à profit de l'empreinte opérationnelle, de l'expertise et de la présence régionale de la DSNP) pourrait appuyer l'élaboration d'un programme de sensibilisation et de formation plus unifié et axé sur les risques, mieux adapté aux réalités opérationnelles et aux besoins des employés à l'échelle de l'Agence. L'amélioration de cette collaboration existante pourrait également contribuer à une utilisation plus stratégique des ressources, en l'harmonisant avec les efforts déployés à l'échelle de l'Agence pour améliorer l'efficacité et soutenir la responsabilité financière.

Mesure du rendement

Reconnaissant la sensibilisation à la sécurité et la formation comme un contrôle clé de la PSG, la Directive sur la gestion de la sécurité exige une mesure continue du rendement ainsi que des mesures correctives pour favoriser l'amélioration continue des programmes de sécurité ministériels.

Compte tenu de la valeur des activités d'évaluation du rendement mesurables et axées sur le comportement, les campagnes de simulation d'hameçonnage sont considérées comme des méthodes efficaces d'évaluation de la sensibilisation des employés à la cybersécurité et de la posture de l'Agence dans ce domaine contre les menaces en ligne. Comme l'Agence avait peu d'activités de mesure du rendement global en place, la vérification a examiné l'étendue et la fréquence des simulations d'hameçonnage comme indicateur clé.

- [caviardé]

Les activités ou les processus d'évaluation limités, comme les campagnes de simulation d'hameçonnage, représentaient une lacune dans la capacité de l'Agence à évaluer l'efficacité de ses efforts en matière de sensibilisation à la cybersécurité et de formation. Sans des mécanismes d'évaluation réguliers et structurés, il était difficile pour l'Agence de déterminer si ses objectifs en matière de sensibilisation et de formation étaient atteints ou si ses stratégies, ses plans et ses initiatives devaient être ajustés pour refléter les besoins organisationnels et des risques changeants en matière de cybersécurité.

L'efficacité des opérations sécurisées de l'Agence dépend en partie du niveau de sensibilisation à la cybersécurité parmi les employés, grâce à un programme de formation bien intégré. L'absence d'un tel programme peut limiter la capacité des employés à reconnaître les cybermenaces et à y réagir de façon appropriée, ce qui augmente le risque de perturbation opérationnelle. Les lacunes dans la sensibilisation peuvent également accroître le risque de menaces internes – que ce soit par négligence ou par des actions malveillantes – en limitant la compréhension qu'ont les employés des comportements sécuritaires et des attentes de l'organisation. Les faiblesses dans la sensibilisation à la sécurité d'une organisation peuvent également être exploitées par des acteurs de menace afin d'obtenir un accès non autorisé ou de lancer des attaques plus vastes à l'échelle des ministères et des systèmes interconnectés.

Annexe A : Critères d'audit

Secteurs d'intérêt	Critères d'audit
1. Gouvernance et gestion des risques	1.1 Les rôles et les responsabilités ministériels en matière de cybersécurité sont bien établis et fonctionnent efficacement. 1.2 Des plans de cybersécurité complets sont en place, en plus de pratiques adéquates de suivi et de production de rapports, pour s'attaquer aux risques liés à lacybersécurité.
2. Contrôles	2.1 L'Agence a mis en place un processus efficace de gestion des événements de cybersécurité pour se préparer aux événements et aux incidents ainsi que pour y réagir rapidement. 2.2 Une culture de sensibilisation à la sécurité est appuyée par une sensibilisation et une formation adaptées.

Annexe B: Méthode d'échantillonnage

Ce qui suit est un aperçu de la méthode d'échantillonnage.

Tests du plan de gestion des événements de cybersécurité

Ce qui a été examiné : La vérification a permis de déterminer si le processus de gestion des événements de cybersécurité de l'Agence était harmonisé avec le PGEC de l'ASFC et du GC. Un échantillon de 30 événements de cybersécurité a été sélectionné et examiné. Ces événements se sont produits entre le 1er avril 2023 et le 30 juin 2024.

Source des données : L'échantillon a été sélectionné à partir des registres de suivi des événements fournis par la DCS. Ces registres comprenaient des métadonnées comme les échéanciers, les emplacements, le statut d'achèvement, le niveau d'incidence et les résultats d'évaluation.

Population et méthode d'échantillonnage : La vérification a appliqué une approche discrétionnaire d'échantillonnage fondée sur les risques pour diviser la population en sous-groupes en fonction des facteurs de risque clés tels que le type d'événement, l'état, la priorité, la composante (par exemple, alertes, avis, hameçonnage/pourriels). Lors de la sélection de l'échantillon final, la vérification a également tenu compte de la couverture globale pour assurer la représentation des différents sous-groupes, dans la mesure du possible.

Parmi la population davantage définie, 30 événements ont été choisis au hasard dans trois équipes de la Division des cyberopérations :

- Équipe d'intervention en cas d'incident : 20 échantillons;
- Équipe de la protection des points d'extrémité et d'intervention : 5 échantillons;
- Centre de cyberdéfense avancé : 5 échantillons.

Tests de vulnérabilité

Ce qui a été examiné : La vérification a examiné les pratiques de gestion des vulnérabilités et des correctifs de sécurité de l'Agence pour ses applications afin d'évaluer la façon dont elles prennent en charge les diverses phases du cycle de vie de la gestion des événements de cybersécurité. Au total, 30 applications ont été examinées pendant la période du 1er avril 2023 au 30 juin 2024.

Source des données : L'échantillon a été sélectionné à l'aide des données obtenues de la Gestion des portefeuilles d'applications et de la Plateforme de collaboration de l'Agence, de concert avec la Division de l'architecture, DGIST.

Population et méthode d'échantillonnage : La vérification a sélectionné un échantillon d'applications nationales et régionales ou locales en utilisant une approche fondée sur le risque (par exemple, prioriser les applications ayant une valeur opérationnelle et une criticité plus élevées), tout en visant à assurer une couverture appropriée dans les différentes directions générales et régions, dans la mesure du possible.

Les responsables de l'audit ont sélectionné un total de 30 applications, y compris :

- Applications nationales de l’ASFC : 20 échantillons ont été sélectionnés à partir des données relatives à la Gestion du portefeuille d’applications de 2023 de l’Agence;
- Applications régionales ou locales de l’ASFC : 10 échantillons ont été sélectionnés à partir du plus récente ensemble de données disponibles dans la Plateforme de collaboration de l’Agence.

Annexe C : Acronymes

ADCS	Agent désigné pour la cybersécurité
AMC	Autoévaluation de la maturité cybernétique
AMOPS	Avis de mise en œuvre de la Politique sur la sécurité
ARC	Agence du revenu du Canada
ASFC	Agence des services frontaliers du Canada
DCS	Direction de la cybersécurité
DGIST	Direction générale de l'information, des sciences et de la technologie
DGRNIP	Direction générale des recours, des normes et de l'intégrité des programmes
DPS	Dirigeant principal de la sécurité
DSNP	Direction de la sécurité et des normes professionnelles
EV	Évaluation des vulnérabilités
GC	Gouvernement du Canada
PGEC	Plan de gestion des événements de cybersécurité
PSG	Politique sur la sécurité du gouvernement
RAA	Rapport après action
RI	Réponse aux incidents
SPC	Services partagés Canada
TI	Technologies de l'information
VP	Vice-président