Direction générale de la vérification et de l'évaluation
Juin 2025

Vérification de la cybersécurité

Anciens Combattants Canada | Veterans Affairs Canada

Canada

Remerciements

L’équipe de vérification tient à remercier les employés de la Direction générale de la technologie de l’information, de la gestion de l’information, de l’administration et de la protection des renseignements personnels d’Anciens Combattants Canada, ainsi que les employés de Services partagés Canada, du Centre de la sécurité des télécommunications et du Centre canadien pour la cybersécurité. Leur apport a été crucial pour la réussite de cette vérification.

Table des matières

Sommaire

Contexte et portée

La menace de cyberattaques présente un risque important et croissant pour les gouvernements du monde entier. Ces menaces peuvent défier la sécurité nationale et la stabilité économique et nuire à la confiance du public. Les cybermenaces peuvent perturber les services essentiels et compromettre des données de nature délicate. Comme ces types d'attaques sont de plus en plus sophistiqués et fréquents et changent rapidement, il est essentiel que les gouvernements investissent continuellement dans des mesures de cybersécurité afin d'atténuer ce risque croissant.

Anciens Combattants Canada (ACC) a la responsabilité de protéger le Ministère contre les cyberattaques et les dommages importants qui pourraient être causés à ses biens et à sa réputation. Le programme de cybersécurité actuel d'ACC vise à « identifier, protéger, détecter, intervenir et rétablir ». Cependant, ACC n'assume pas seul cette responsabilité. Services partagés Canada (SPC) a également un rôle à jouer dans la prestation de certains services à ACC pour répondre à ses besoins en matière de cybersécurité. Aux fins de la présente vérification, il est important de souligner que la vérification porte uniquement sur le rôle d'ACC dans la gestion de la cybersécurité.

C'est la première fois que ce sujet fait l'objet d'une vérification à ACC. Dans cette optique, notre mission s'est concentrée sur la gouvernance, les rôles et responsabilités, les politiques et les procédures. Cette approche est conforme aux directives de l'Institut des vérificateurs internes (IVI) sur la vérification des programmes de cybersécurité. Il est raisonnable de penser qu'une autre vérification de la cybersécurité pourrait être bénéfique dans le futur afin d'examiner les aspects plus techniques de la cybersécurité.

La présente vérification vise à donner l'assurance raisonnable qu'un cadre de contrôle de gestion adéquat est en place pour assurer que le Ministère a clairement défini ses objectifs en matière de cybersécurité et qu'il est prêt à gérer la cybersécurité à l'ère du numérique.

La portée de la vérification comprenait les cadres de contrôle de gestion, les politiques et les procédures qui étaient en place entre le 1er janvier 2023 et le 30 septembre 2024 inclusivement. Toutefois, comme l'équipe de vérification voulait s'assurer que les renseignements disponibles les plus récents étaient analysés, elle n'a pas considéré certains éléments à jour qui ont été réalisés par le Ministère.

Principales constatations

L’équipe de la sécurité des technologies de l’information est l’équipe responsable de la cybersécurité à ACC. Petite, mais extrêmement compétente, elle transmet ses vastes connaissances organisationnelles et repose fortement sur ses compétences et son expérience pour gérer la cybersécurité à ACC. Toutefois, il existe des possibilités d’améliorer le programme de cybersécurité d’ACC.

La structure de gouvernance de la cybersécurité à ACC manque de clarté en ce qui concerne la gouvernance globale et la définition des rôles et des responsabilités. De plus, certaines politiques et procédures sont désuètes et, généralement, elles sont mises à jour uniquement de manière réactive.

ACC n’a pas d’outil central de production de rapports pour consigner et documenter adéquatement les cybermenaces et les vulnérabilités. Il doit s’appuyer sur plusieurs outils différents et la responsabilité est partagée entre les membres de l’équipe, ce qui accroît le risque de manquer des renseignements. Cela peut également constituer une occasion manquée de surveiller, de prévoir et de cerner les tendances de façon efficace afin de mettre à profit sa position future à l’égard de la cybersécurité.

L’équipe de vérification a constaté qu’un nouveau cours sur la cybersécurité est devenu obligatoire pour tous les employés en janvier 2025 et que, grâce à la campagne de sensibilisation à l’hameçonnage menée par ACC, les employés reconnaissent maintenant de plus en plus les courriels d’hameçonnage.

Le Centre canadien pour la cybersécurité (CCC) est la seule source unifiée qui offre à la population canadienne des conseils d’experts, des avis, des services et un soutien en matière de cybersécurité. Il offre une vaste gamme de services et d’outils. Bien qu’ACC en utilise certains de ces outils et services, l’équipe de vérification a déterminé qu’ACC devrait envisager de tirer parti d’un plus grand nombre de ces outils et services à l’avenir.

Conclusion

Dans l’ensemble, l’équipe de vérification a conclu qu’ACC bénéficiait d’une solide réputation auprès des autres ministères pour ce qui est de la cybersécurité, cependant, il est possible d’apporter d’autres améliorations.

Principales recommandations

L’équipe de vérification a recommandé que le Ministère élabore un cadre de gouvernance officiel qui comprend les rôles et les responsabilités en matière de

cybersécurité à ACC, et qu'il détermine la formation requise pour les employés. Une autre recommandation a été formulée afin d'assurer que le Ministère met à profit de nouveaux outils et les outils existants, en particulier ceux offerts par le CCC, pour appuyer l'atténuation des risques de cybermenaces. Enfin, l'équipe de vérification recommande que les recommandations découlant de l'exercice de simulation de cyberattaque soient mises en œuvre en temps opportun.

Signature de la dirigeante principale de la vérification
Lindy McQuillan, CPA, CMA
Dirigeante principale de la vérification
Anciens Combattants Canada

1.0 Contexte

Le Centre de la sécurité des télécommunications (CST) définit la cybersécurité comme l'ensemble des technologies, procédures et pratiques conçues pour protéger les réseaux,
les appareils, les programmes et les données contre les attaques, les dommages ou les accès non autorisés.

La cybersécurité retient de plus en plus l'attention des conseils et comités de direction, car la connectivité de réseau continue d'augmenter à une rapidité fulgurante et fait en sorte que les résultats opérationnels sont exposés à un risque accru. Par conséquent, la fonction de vérification est de plus en plus nécessaire pour mener des évaluations de la conformité en matière de cybersécurité, valider l'acceptation des risques de façon officielle, mener des essais sur les contrôles internes et appuyer les enquêtes de cybersécurité et judiciaires.

Les incidents de cybersécurité touchant les systèmes informatiques du gouvernement du Canada (GC) peuvent avoir une incidence importante sur l'exécution des programmes et des services gouvernementaux destinés aux Canadiens et, par conséquent, sur la confiance accordée au gouvernement. La sécurité du gouvernement et la continuité de ses programmes et services reposent sur la capacité des ministères et organismes et du gouvernement dans son ensemble à gérer les incidents de cybersécurité. La capacité d'intervenir de manière uniforme, coordonnée et rapide à l'échelle du gouvernement en cas d'incident de cybersécurité est essentielle afin d'assurer la sécurité et la résilience dans l'exécution des programmes et des services du GC.

Conformément aux nouvelles directives et normes établies par l'Institut des vérificateurs internes (IVI), en vigueur depuis le 9 janvier 2025, l'équipe de vérification a adopté une approche descendante de l'industrie pour le premier engagement d'ACC à l'égard de la cybersécurité. Le 30 octobre 2024, l'équipe de vérification a assisté à la Conférence sur la cybersécurité de l'IVI pour en apprendre davantage sur la structure, et a concentré

son attention sur la gouvernance et l'intervention en cas d'incident, ainsi que sur les politiques et procédures appropriées.

Lorsqu'ACC détermine que des services sont requis pour appuyer des initiatives de cybersécurité, le rôle de Services partagés Canada (SPC) consiste à soutenir ACC en lui fournissant les logiciels, les systèmes et les ressources nécessaires pour la tâche à accomplir. SPC collabore avec l'équipe de la sécurité des technologies de l'information d'ACC pour veiller à ce que les filtres antipourriels et autres mécanismes de protection soient configurés de façon efficace et conformément aux politiques relatives à la sécurité. SPC intervient également lorsque des incidents majeurs surviennent afin de s'assurer que le niveau de protection des systèmes et logiciels actuels est suffisant pour atténuer les risques, et aide ACC à obtenir ce dont il a besoin pour résoudre le problème.

À ACC, chacun a la responsabilité de protéger le réseau d'ACC des incidents de cybersécurité, car cela pourrait causer de graves dommages aux biens et à la réputation du Ministère. En outre, en raison de l'adoption et de l'utilisation croissantes de l'intelligence artificielle (IA) à l'échelle mondiale, il deviendra de plus en plus difficile d'assumer cette responsabilité. Le programme de cybersécurité actuel d'ACC vise à « identifier, protéger, détecter, intervenir et rétablir ». Dans cette optique, ACC n'a pas encore eu d'incident « majeur » connu.

2.0 Résultats de la vérification

2.1 Structure de gouvernance

La structure de gouvernance de la cybersécurité à ACC devrait être mieux définie et mieux documentée.

Pourquoi est-ce important?

Une structure de gouvernance bien documentée et bien comprise est importante, car elle établit des lignes directrices claires pour tous les employés d'ACC afin qu'ils puissent se conformer aux exigences de sécurité et assurer la résilience dans l'environnement numérique. Elle permet également d'assurer que le Ministère est prêt à intervenir en cas d'incident de cybersécurité et que les risques sont atténués de manière à réduire les atteintes possibles à la sécurité ou la perte potentielle de données.

Ce que nous avons constaté

L'équipe de vérification a déterminé qu'ACC n'avait pas de structure de gouvernance bien définie en ce qui concerne la prise de décision en matière de cybersécurité. De plus, les politiques et procédures internes ne sont pas bien comprises et bien documentées ou ne sont pas mises à jour de manière uniforme, et ACC n'a pas établi d'indicateurs de rendement clés ou n'assure pas la mesure ou le suivi du rendement.

Les entretiens avec les répondants clés ont révélé que les politiques et procédures étaient la plupart du temps mises à jour que de manière réactive lorsque des employés remarquent que certains documents figurant dans leur répertoire GCdocs sont désuets. La responsabilité de mettre à jour ces documents est partagée entre les membres de l'équipe de la sécurité des technologies de l'information. L'équipe de vérification a également constaté que la plupart des renseignements figurant sur le site intranet d'ACC étaient périmés ou désuets.

Le programme de cybersécurité d'ACC repose sur plusieurs intervenants. Services partagés Canada (SPC) joue un rôle dans le soutien des réseaux et des systèmes d'ACC, tout comme le chef du service de sécurité du Ministère en ce qui concerne le signalement des incidents majeurs aux autorités appropriées. Cependant, la grande majorité du programme est dirigée par l'équipe de la sécurité des technologies de l'information, qui est petite, mais extrêmement compétente, et qui fait partie de la Direction générale de la technologie de l'information, de la gestion de l'information, de l'administration et de la protection des renseignements personnels.

L'équipe de la sécurité des technologies de l'information est composée de six employés qui jouent chacun un rôle important dans la position du Ministère en matière de cybersécurité. Elle comprend un gestionnaire de TI, un conseiller technique en TI, trois analystes en TI et un technicien en TI. Le rôle de chef d'équipe existe, mais n'est pas financé, de sorte que le seul poste de supervision est celui de gestionnaire. Les membres de l'équipe possèdent une vaste expérience et comprennent leurs rôles et leurs responsabilités malgré le fait qu'ils ne sont pas toujours documentés ou mis à jour. Les entretiens avec les répondants clés ont révélé que les rôles et responsabilités en matière de cybersécurité n'étaient pas bien compris en dehors de l'équipe.

L'équipe de vérification a conclu qu'ACC respectait son plan de gestion des événements de cybersécurité (PGEC), de même que les lignes directrices du CCCS et les politiques du Conseil du Trésor relatives à la cybersécurité. Elle reconnaît que cela représente une grande quantité d'information à traiter et à gérer et que l'équipe de la sécurité des technologies de l'information parvient à mener à bien son travail malgré les lacunes dans la structure de gouvernance globale.

Au moment de la vérification, ACC n'avait pas encore eu d'incident de cybersécurité « majeur » connu, qui est défini comme tout événement, acte, omission ou situation qui pourrait porter atteinte à la sécurité du gouvernement, y compris les menaces, les vulnérabilités et les incidents de sécurité. L'expérience de l'équipe de la sécurité des technologies de l'information, les programmes de correctifs réguliers, les mises à jour logicielles, les campagnes de sensibilisation, comme l'envoi de faux courriels d'hameçonnage, ainsi que la formation connexe ont joué un rôle important dans la protection du Ministère contre les incidents de cybersécurité.

Quelles sont les répercussions?

Les incidents de cybersécurité peuvent avoir une incidence considérable sur le Ministère, compromettre l'intégrité des données des clients et accroître le risque de perte financière ou de réputation. Dans cette optique, il faut reconnaître qu'ACC sera toujours exposé au risque d'un incident de cybersécurité, surtout si l'on considère l'adoption croissante de l'IA à l'échelle mondiale et d'autres facteurs.

ACC doit s'assurer que des mesures d'atténuation sont en place pour appuyer tous les employés et protéger le Ministère. Malgré le manque de structure de gouvernance documentée sur la cybersécurité, ACC réussit à gérer les exigences des diverses politiques et lignes directrices. Toutefois, advenant un roulement de personnel, cela risque de ne plus être le cas et le fait d'avoir une solide structure de gouvernance permettrait d'atténuer ce risque.

2.2 Formation

La formation peut jouer un rôle essentiel en aidant les employés à comprendre leurs rôles et responsabilités en matière de cybersécurité, compte tenu de la nature technique de celle-ci et du rythme des changements dans ce domaine.

Les employés de la sécurité des technologies de l'information peuvent également avoir besoin d'une formation plus spécialisée pour être en mesure de s'adapter à l'environnement numérique en constante évolution et de composer avec la hausse des cybermenaces, mais leurs responsabilités actuelles peuvent constituer un obstacle à leur participation à une telle formation.

Pourquoi est-ce important?

Comme le domaine des technologies de l'information et les menaces à la cybersécurité qui en découlent continuent d'évoluer rapidement, il est essentiel que tous les employés d'ACC soient bien informés et reçoivent une formation appropriée sur la cybersécurité. De plus, il est crucial que les employés de la sécurité des technologies de l'information demeurent à jour dans la formation sur la cybersécurité, car le contexte des menaces continue d'évoluer rapidement et il y a de nombreuses nouvelles vulnérabilités et méthodes d'attaque qui émergent. Le fait d'être formé de façon adéquate constitue un autre facteur important qu'ACC doit prendre en considération pour atténuer les risques liés à la cybersécurité.

Ce que nous avons constaté

L'équipe de vérification a examiné la formation offerte à tous les employés d'ACC et celle offerte aux employés de la sécurité des technologies de l'information.

Le 22 janvier 2025, pendant le déroulement de la vérification, ACC a mis en œuvre son premier cours obligatoire sur la cybersécurité (Découvrez la cybersécurité [DDN235])

pour tous les employés d'ACC. Ce cours obligatoire devait être suivi avant le 31 mars 2025 et chaque année par la suite. Le cours a été établi par le dirigeant principal de l'information du Secrétariat du Conseil du Trésor et est offert par l'École de la fonction publique du Canada (EFPC), en collaboration avec le Centre canadien pour la cybersécurité.

Au moment de la vérification, il était prévu que l'achèvement du cours ferait l'objet d'un suivi comme pour les autres cours obligatoires et que le cours serait examiné et mis à jour au moins une fois par an. Les mises à jour seront alimentées par le contexte des cybermenaces en constante évolution et les commentaires reçus des apprenants. L'équipe de vérification a suivi le cours relativement bref et a estimé qu'il avait eu une incidence considérable sur sa connaissance des pratiques exemplaires en matière de cybersécurité.

ACC a également mis en œuvre une campagne de sensibilisation à l'hameçonnage dans le cadre de laquelle de faux courriels d'hameçonnage sont envoyés aux employés afin de les sensibiliser aux pratiques exemplaires en matière de cybersécurité. Les employés qui « échouent » ce test reçoivent un avis les informant qu'ils doivent suivre deux cours liés à la cybersécurité et réussir le bref questionnaire final qui suit chaque cours. Si l'employé n'obtient pas une note de 80 % ou plus, il doit reprendre le questionnaire. Lors des entretiens, les répondants clés ont laissé entendre que, grâce à cette campagne, les employés d'ACC reconnaissaient plus facilement les courriels d'hameçonnage et étaient plus nombreux à les signaler. Toutefois, il est possible de mettre à profit ces données pour cerner les tendances et cibler les futures campagnes en fonction de ces tendances. De plus, il est également possible de modifier le questionnaire lors des essais subséquents afin d'assurer que les employés acquièrent activement les connaissances nécessaires.

L'équipe de vérification a constaté qu'une large gamme de formations s'offraient à l'équipe de la sécurité des technologies de l'information d'ACC. Celle-ci a accès à des cours gratuits offerts par Microsoft et à certains cours qui correspondent au rôle ou au domaine d'intérêt des membres de l'équipe. Le programme de formation de l'équipe n'est pas très vaste, surtout en ce qui concerne la formation obligatoire, et il ne fait pas l'objet d'un suivi officiel dans un emplacement central. Les employés ont mentionné que la direction les encourageait à suivre la formation afin d'appuyer l'apprentissage et le perfectionnement des autres employés. Cependant, les entretiens ont révélé que la formation pouvait souvent être retardée ou annulée en raison de priorités concurrentes qui empêchaient les employés de suivre la formation requise.

Quelles sont les répercussions?

Le Ministère a pris des mesures en vue d'améliorer la sensibilisation et la formation offerte aux employés d'ACC en instaurant le premier cours obligatoire sur la cybersécurité, mais l'absence de mesures pour améliorer et mettre à jour régulièrement les initiatives de formation sur la cybersécurité pourrait avoir de graves conséquences pour le Ministère. Sans une formation appropriée, les employés, en particulier ceux qui assument un rôle lié à la sécurité des technologies de l'information, pourraient ne pas

être en mesure de reconnaître une cybermenace ou d'intervenir de façon appropriée, ce qui pourrait accroître le risque pour le Ministère. Dans cet environnement qui évolue rapidement, les employés de la sécurité des technologies de l'information doivent demeurer à jour dans leur formation et celle-ci devrait faire l'objet d'un suivi pour assurer que tous les cours nécessaires ont été suivis.

Recommandation 1

Il est recommandé que le sous-ministre adjoint, Secteur de la dirigeante principale des finances et des services ministériels, élabore un cadre de gouvernance officiel pour la cybersécurité qui comprend notamment :

- les rôles et les responsabilités;
- la formation obligatoire et les activités de sensibilisation.

Réponse de la direction

La direction approuve en partie cette recommandation.

Cadre de gouvernance de la cybersécurité et rôles et responsabilités connexes

La Direction générale de la technologie de l'information, de la gestion de l'information, de l'administration et de la protection des renseignements personnels rendra officiel son cadre de gouvernance de la cybersécurité, y compris les rôles et les responsabilités. La gouvernance actuelle relève du Conseil consultatif sur le numérique, et c'est par l'entremise de ce dernier que nous établirons d'autres rapports de haut niveau. Nous documenterons également de façon officielle les principaux rôles et responsabilités en matière de cybersécurité qui ne sont pas suffisamment documentés dans les instruments de politique du Secrétariat du Conseil du Trésor (SCT). Ce cadre sera conforme à la *Politique sur la sécurité du gouvernement* et à la *Politique sur les services et le numérique* du SCT.

Formation et sensibilisation

Comme il a été mentionné, le Ministère a mis en œuvre une formation obligatoire pour les employés. Cette formation, qui est offerte par l'École de la fonction publique du Canada, sera gérée et régulièrement mise à jour par l'École en fonction des besoins du gouvernement du Canada. Le Ministère pourra ainsi s'assurer que la formation est impérative et à jour à l'avenir.

En ce qui concerne la formation des employés, le Ministère n'établira pas de plan de formation normalisé pour les employés de la sécurité des technologies de l'information et laissera au gestionnaire de l'unité le soin de gérer la formation selon ses besoins et ses objectifs. Le choix de cette approche repose sur les facteurs suivants :

1. Une formation offerte à un petit groupe d'employés serait gérée plus efficacement par le gestionnaire qui est en contact direct avec ces employés.
2. Le contexte de la sécurité évolue rapidement et la formation doit pouvoir être modifiée en fonction des impératifs de sécurité actuels.

Les employés ont des objectifs différents et la formation doit correspondre à leur rôle et à leurs besoins.

2.3 Surveillance et signalement des cybermenaces et des vulnérabilités

Différents canaux et outils sont actuellement en place pour évaluer, mettre à jour et signaler les problèmes potentiels, mais il n'existe pas d'outil central de production de rapports.

Pourquoi est-ce important?

Une surveillance précise et efficace pour le signalement des cybermenaces et des vulnérabilités potentielles est importante, car elle aide à cerner les cyberévénements et les tendances. Elle fournit également à la haute direction un portrait précis de la situation actuelle d'ACC en matière de cybersécurité. Alors que la cybersécurité continue d'évoluer avec l'utilisation croissante d'outils comme l'intelligence artificielle et notre dépendance accrue aux services numériques, il est important qu'ACC intègre des outils novateurs pour rester efficient et efficace dans la prévention, la détection et l'atténuation des risques.

Ce que nous avons constaté

La vérification a révélé qu'ACC prend des mesures pour surveiller et signaler les cybermenaces et les vulnérabilités, bien qu'il y ait des points à améliorer. Par exemple, le Centre de la sécurité des télécommunications (CST) a défini les « 10 meilleures mesures de sécurité des TI » à la suite d'une analyse des tendances en matière de cybermenaces touchant les réseaux connectés à Internet du GC. Essentiellement, il y a dix choses qu'un ministère devrait faire pour aider à atténuer les menaces à la cybersécurité. L'équipe de vérification a confirmé qu'ACC suit tous ces éléments et prend donc des mesures importantes pour protéger son réseau et ses biens.

L'équipe de vérification a également pu observer l'équipe de sécurité de la technologie de l'information passer en revue plusieurs systèmes différents qu'elle doit surveiller quotidiennement. L'équipe de sécurité de la technologie de l'information partage collectivement la responsabilité, sans qu'aucun poste précis ne soit clairement attribué à la tâche de surveillance de ces systèmes, ce qui pourrait augmenter le risque qu'une menace ne soit pas détectée.

En raison de l'obligation de surveiller plusieurs systèmes différents, il est à noter que l'équipe de sécurité de la technologie de l'information ne dispose pas d'un outil central de production de rapports. Plusieurs ressources et outils sont utilisés pour gérer, surveiller et signaler les menaces à la cybersécurité. Ces menaces et vulnérabilités sont cernées par plusieurs canaux, tels que les courriels, les alertes Microsoft, le CCC et d'autres tableaux de bord internes. L'équipe de sécurité de la technologie de l'information doit extraire manuellement des données de divers systèmes pour en faire rapport à la haute direction, au besoin.

Le CCC offre de nombreux services aux ministères du GC, mais seulement deux d'entre eux sont actuellement obligatoires. Les services obligatoires sont le programme de capteurs et le Service national de notification de cybermenace (SNNC). L'équipe de vérification a constaté qu'ACC est abonné aux deux services obligatoires. Elle a également constaté qu'ACC est abonné à la plupart des autres outils offerts par le CCC, mais qu'ACC ne dispose pas des ressources nécessaires pour tirer pleinement parti de ces services supplémentaires, car il y en a environ 30 à envisager.

Par exemple, un service non obligatoire cerné par le CCC est un tableau de bord appelé Howler qui est conçu pour consolider les alertes de toutes les sources et différencier celles qui nécessitent un triage ou non. Les ingénieurs de détection sont censés normaliser les alertes, afin qu'elles puissent être consultées et comparées à un schéma commun : Elastic Common Schema (ECS). En regroupant toutes les alertes au même endroit sous un seul schéma, il est beaucoup plus facile de trouver des événements corrélés qui méritent un examen minutieux de la part d'un analyste du triage. Par exemple, un analyste peut facilement trouver toutes les alertes liées à une adresse IP source donnée avec un seul critère de filtrage, quel que soit le schéma de la télémétrie d'origine. De même, il existe d'autres produits, comme Microsoft Sentinel, qui fourniraient un type de service semblable.

Quelles sont les répercussions?

Travailler avec plusieurs outils peut être difficile à gérer, augmente les risques d'erreur humaine et risque d'empêcher un cyberévénement de se produire. De plus, lorsque des données et des renseignements sont extraits manuellement de divers systèmes pour faire rapport à la haute direction ou à d'autres personnes, il est possible que certaines données soient omises par inadvertance. Comme personne n'est spécifiquement affecté à cette responsabilité, il y a un risque que des événements soient manqués.

De plus, en l'absence d'une méthode centralisée pour rendre compte des menaces et des vulnérabilités, il se peut que l'on rate une occasion de cerner et de surveiller les tendances qui pourraient accroître l'atténuation des risques du Ministère.

Recommandation 2

Il est recommandé que le sous-ministre adjoint du Secteur du dirigeant principal des finances et des services ministériels s'assure que le réseau d'ACC est efficacement protégé et surveillé en permanence contre les menaces potentielles :

- en élaborant et en mettant en œuvre des processus et des procédures visant à surveiller adéquatement le réseau d'ACC et les appareils connectés;
- en explorant la possibilité d'intégrer un outil central de production de rapports;
- en effectuant une analyse des services supplémentaires du CCC et en mettant en place ceux qui sont jugés avantageux pour ACC.

Réponse de la direction

La direction est d'accord avec cette recommandation.

Analyse de l'environnement et faisabilité de l'outil

L'équipe de sécurité de la TI examinera et documentera les procédures et les sources surveillées pour la sécurité du réseau d'ACC et des appareils connectés afin d'assurer l'uniformité et la continuité des activités. Elle examinera également les sources pour s'assurer qu'il n'y a pas de chevauchement entre ACC et les partenaires de sécurité. En fonction de ces résultats, l'équipe déterminera les exigences à suivre et si un outil est nécessaire et faisable, et si c'est le cas, mettra en œuvre cet outil.

Évaluation des services de Mon cyberportail

L'équipe de sécurité de la TI évaluera les systèmes et les services offerts par l'entremise de Mon cyberportail. Si un service est jugé avantageux pour le Ministère et que des ressources internes suffisantes sont disponibles pour soutenir son utilisation, la Sécurité de la TI s'abonnera au service.

2.4 Gestion des événements de cybersécurité d'ACC

En mars 2024, une entreprise de consultation indépendante a été invitée à participer à la mise à l'essai du Plan de gestion des événements de cybersécurité (PGEC) d'ACC. Dans le cadre de cet exercice, dix recommandations ont été documentées, mais aucun progrès n'a été réalisé quant à leur mise en œuvre.

Pourquoi est-ce important?

L'objectif de cet exercice était de donner un aperçu de l'état de préparation du Ministère à une éventuelle compromission ou à un événement de cybersécurité. ACC doit être prêt à intervenir et à gérer les répercussions et les conséquences de l'événement, et

toutes les personnes concernées doivent bien comprendre leur rôle et leurs responsabilités ainsi que les processus connexes.

La réalisation de ce type d'exercice est une partie très importante de la gestion de la cybersécurité. C'est une façon de renforcer la résilience organisationnelle en s'assurant qu'en cas d'incident réel, l'intervention du Ministère est coordonnée, efficiente et efficace. En fin de compte, le fait d'avoir une réponse efficace réduira le risque de dommages financiers, opérationnels et réputationnels.

Ce que nous avons constaté

En mars 2024, ACC a invité une entreprise tierce à participer à la mise à l'essai du Plan de gestion des événements de cybersécurité (PGEC) d'ACC. Cet exercice traitait d'une possible compromission de la cybersécurité et d'une demande de rançon afin de donner un aperçu de l'état de préparation d'ACC aux menaces réelles et de cerner les possibilités d'amélioration. L'exercice a mobilisé des participants au niveau de la haute direction [ACC, SCT, SSC, Tribunal des anciens combattants (révision et appel)] qui seraient impliqués d'une manière ou d'une autre dans un cyberévénement au sein d'ACC.

À la suite de cet exercice, un rapport a été rédigé et dix recommandations ont été documentées pour aider à améliorer la posture de cybersécurité de l'équipe de sécurité de la technologie de l'information. Voici les trois principales recommandations découlant de cet exercice :

1. Élaborer une matrice qui décrit les principaux rôles et responsabilités des participants (y compris les tiers et les partenaires) dans l'intervention en cas de cyberattaque et l'inclure dans le PGEC.

2. Clairement identifier le décideur approprié à chaque étape de la réponse et s'assurer qu'il a le pouvoir d'agir. **Remarque importante :** Il n'y avait pas suffisamment de clarté sur les procédures d'acheminement aux échelons supérieurs et sur le moment où il fallait acheminer un événement au cours de cet exercice.

3. Mettre à jour les plans : Continuellement élaborer, mettre à l'essai et peaufiner le PGEC global. Documenter les plans de scénarios de cybersécurité et peaufiner les manuels relatifs aux systèmes informatiques et s'assurer que les PCA sont mis à jour en conséquence.

L'équipe de vérification a examiné la documentation disponible relative à cet exercice et a constaté qu'aucun progrès n'a été réalisé à ce jour en ce qui concerne la mise en œuvre de ces recommandations. L'équipe de sécurité de la technologie de l'information a déclaré que cela était dû à de multiples priorités concurrentes et à un manque de ressources disponibles pour se concentrer sur la mise en œuvre – Les entrevues avec les informateurs clés ont suggéré que cet exercice pourrait également devenir un événement régulier afin de s'assurer qu'ACC était bien préparé à un incident. La

vérification a permis de constater qu'il n'existe actuellement aucun plan documenté pour un exercice de suivi.

Quelles sont les répercussions?

La réalisation de ce type d'exercice a fourni à toutes les personnes concernées des informations précieuses sur leurs rôles et responsabilités en cas de cyberattaque réelle. L'exercice a également aidé les participants à évaluer leur état de préparation, à acquérir plus d'expérience et à cerner les domaines à améliorer.

Cet exercice a permis de documenter dix recommandations visant à améliorer l'état de préparation du Ministère. Toutefois, s'il ne donne pas suite aux recommandations de l'exercice du PGEC en temps opportun ou s'il ne mène pas ce type d'exercice à intervalles réguliers, le Ministère risque davantage de ne pas être préparé en cas de cyberévénement et de perdre l'avantage de la précieuse expérience acquise grâce à un tel exercice.

Recommandation 3

Il est recommandé que le sous-ministre adjoint du Secteur du dirigeant principal des finances et des services ministériels prend des mesures pour atténuer les risques de cybersécurité :

- en élaborant un plan d'action pour mettre en œuvre les recommandations existantes issues de l'exercice du PGEC avec un calendrier de mise en œuvre connexe;
- en créant un plan pour mener des exercices supplémentaires sur le PGEC à intervalles réguliers avec un mécanisme pour assurer la mise en œuvre des recommandations qui en découlent en temps opportun.

Réponse de la direction

La direction est partiellement d'accord avec cette recommandation.

Recommandations découlant du PGEC :

La Direction du cyber, de la gestion de l'information et des services de données mettra en œuvre les recommandations 1, 2 et 4.

- Les recommandations 1 et 2 impliquent la création d'une matrice des rôles et des responsabilités qui indique les décideurs clés.
- La recommandation 4 implique la réalisation d'un exercice du PGEC tous les deux ans.

Aucune autre mesure ne sera prise pour la recommandation suivante :

- La recommandation 3 est liée à la tenue à jour de la documentation pour le PGEC et le PCA, ce qui sera fait au moyen d'exercices menés tous les deux ans et de processus du PCA.
- La recommandation 5 décrit la préparation de conseils sur les mesures de soutien aux clients pour lesquelles le Ministère demanderait des conseils et des directives au CCC et au SCT. Par conséquent, nous n'élaborerions pas nos propres procédures et conseils pour ce point.
- La recommandation 6 relative à la propension au risque en général continuera de faire l'objet d'un examen minutieux et d'un taux de réponse élevé, comme l'indiquent le cadre ministériel de gestion des risques et la position actuelle du gouvernement du Canada sur la cybersécurité. Les éléments de risque feront l'objet de discussions dans le cadre de mises à jour sur la gouvernance ainsi que de séances d'information situationnelles qui auront lieu dans le cadre de la nouvelle gouvernance et, par conséquent, nous ne participerons pas à un exercice distinct.
- La recommandation 7 concernant les modèles de communication n'aurait pas suffisamment d'avantages, car les communications dépendront grandement du scénario et de nombreuses situations uniques. Les communications seront guidées par le CCC et le SCT pour les scénarios plus complexes, et pour quelque chose de peu fréquent, il en résultera un lourd fardeau de tenir le matériel constamment à jour pour un avantage minime.
- La recommandation 8 concernant les menaces internes par rapport aux menaces externes est prise en compte dans toutes les situations et fait partie des connaissances et des pratiques courantes en matière de sécurité.
- La recommandation 9 relative à la saisie des dossiers d'incidents est décrite à plusieurs reprises dans les modèles du PGEC et est intégrée au processus. Il n'y a pas beaucoup d'avantages à offrir une formation spécifique aux personnes sur la saisie de notes, car il peut s'agir de plusieurs personnes et il s'agit généralement d'une pratique courante.
- La recommandation 10 est une considération notée concernant le confinement par rapport à l'élimination et ferait partie des considérations normalisées d'un analyste de la cybersécurité. Aucune mesure supplémentaire ne serait nécessaire.

2.5 Opinion de l'équipe de vérification

En se fondant sur les constatations ci-dessus, l'équipe de vérification a déterminé que la gestion de la cybersécurité à ACC doit être améliorée. Bien qu'ACC accomplisse actuellement de nombreuses tâches essentielles à l'atténuation des cybermenaces pour le Ministère, des améliorations, telles qu'un cadre de gouvernance officiel qui décrit les rôles et les responsabilités ainsi que les exigences en matière de formation, l'utilisation d'outils et de ressources nouveaux et existants, la réalisation régulière d'un exercice simulé de cybersécurité et l'engagement à mettre en œuvre les

recommandations découlant de l’exercice aideront à s’assurer que le Ministère est bien positionné pour relever les défis associés à la cybersécurité à l’avenir.

De plus, étant donné que c’est la première fois que ce sujet fait l’objet d’une vérification à ACC, la cybersécurité devrait être prise en compte à l’avenir dans le cadre de la planification d’une vérification fondée sur les risques pour une vérification supplémentaire, peut-être d’un point de vue plus technique.

La vérification est conforme aux Normes internationales pour la pratique professionnelle de l’audit interne de l’Institut des auditeurs internes (les Normes), comme en témoignent les résultats du programme d’assurance et d’amélioration de la qualité. Les constatations et conclusions de la vérification contenues dans le présent rapport sont fondées sur des éléments probants suffisants et appropriés recueillis conformément aux Normes. Les opinions exprimées dans le présent rapport sont fondées sur les conditions qui existaient au moment de la vérification et ne s’appliquent qu’à l’entité examinée.

Annexe A – Au sujet de la vérification

Portée et objectifs

La portée de la vérification comprenait les cadres, les politiques et les procédures de contrôle de gestion en place du 1er janvier 2023 au 30 septembre 2024 inclusivement. Il était très important d'analyser les dernières informations disponibles compte tenu de l'évolution rapide du paysage de la cybersécurité. La portée excluait les contrôles d'accès au système, car une vérification distincte en est à ses dernières étapes.

Les objectifs de la présente vérification étaient les suivants :

1. ACC dispose d'une structure de gouvernance, de politiques, de procédures et d'une surveillance appropriées pour gérer la cybersécurité en fonction des lignes directrices et des pratiques exemplaires du GC; et
2. ACC a mis en place les mesures appropriées pour prévenir un cyberévénement, y réagir et en tirer des leçons.

Critères de la vérification

Objectif 1

ACC dispose d'une structure de gouvernance, de politiques, de procédures et d'une surveillance appropriées pour gérer la cybersécurité en fonction des lignes directrices et des pratiques exemplaires du GC.

Critères

a) Le Ministère a mis en œuvre un cadre de gouvernance efficace et a mis en place des organes pour assurer une surveillance suffisante des risques et des initiatives en matière de cybersécurité.

b) Le Ministère a clairement défini et communiqué les rôles, les responsabilités, les politiques et les procédures liés à la cybersécurité, y compris les rôles et les responsabilités clairement définis avec des partenaires externes, tels que Services partagés Canada et le Centre canadien pour la cybersécurité.

c) Le Ministère a mis en place un processus de surveillance du rendement et d'établissement de rapports pour évaluer et mettre à jour les activités de cybersécurité et en rendre compte.

d) Le Ministère fournit la formation et les ressources nécessaires pour aider les employés à s'acquitter de leurs responsabilités en matière de cybersécurité.

Objectif 2

ACC a mis en place les mesures appropriées pour prévenir un cyberévénement, y réagir et en tirer des leçons.

Critères

a) Le Ministère fournit la formation, les outils, les ressources et les renseignements nécessaires pour aider les employés à s'acquitter de leurs responsabilités en matière de cybersécurité.

b) Le Ministère a mis en place les processus et les procédures nécessaires pour prévenir une cyberattaque et intervenir en cas de cyberattaque.

c) Le Ministère a mis en place un processus de surveillance du rendement et d'établissement de rapports pour évaluer et mettre à jour les activités de cybersécurité et en rendre compte.

Méthodologie

Méthode	Objectif
Entrevues	Obtenir des renseignements sur les rôles et responsabilités des personnes interrogées ainsi que de SPC et du CCC. Obtenir des renseignements sur les politiques, les processus, les lignes directrices et les normes en place et déterminer s'ils sont à jour. Obtenir des renseignements sur la formation de l'équipe de sécurité de la technologie de l'information qui est responsable de la cybersécurité à ACC ainsi que sur la formation de tous les employés. Obtenir des renseignements sur le suivi, la surveillance et le signalement d'événements, d'incidents et de tendances relatifs à la cybersécurité. Obtenir des renseignements sur les systèmes et les logiciels utilisés pour protéger les biens d'ACC d'événements de cybersécurité. Obtenir des renseignements sur la documentation désuète sur ACC au tr@vail ainsi que sur le processus de documentation général. Obtenir des renseignements sur les simulations de cyberévénements menées comme expérience d'apprentissage et protocole de sécurité.
Observation directe	L'équipe de vérification a suivi le cours Découvrez la cybersécurité – DDN235, obligatoire pour tous les employés. (entré en vigueur en janvier 2025)

Méthode	Objectif
	L'équipe de vérification a passé en revue le processus de signalement de courriels d'hameçonnage, réussissant et échouant au questionnaire et quels ont été les résultats. Observer les divers processus système que l'équipe de sécurité de la technologie de l'information d'ACC utilise.
Examen de la documentation	Examiner les plans de gestion des événements de cybersécurité du GC et d'ACC. Examiner les renseignements sur les services, les outils et autre se trouvant sur le site Web du CCC. Examiner la Stratégie intégrée de cybersécurité du GC. Examiner les renseignements sur la sécurité de la technologie de l'information se trouvant sur l'intranet d'ACC (ACC au tr@vail). Examiner les articles dans les médias. Examiner plusieurs politiques, directives, processus, lignes directrices, normes et plans de sécurité (SCT, CCC, ACC, GC). Examiner les vérifications internes et externes et les évaluations horizontales effectuées par le passé et en cours. Examiner les présentations sur le signalement d'attaques de cybersécurité simulées.
Examen des dossiers	S.O.
Analyse des données	S.O.
Sondage et questionnaire	S.O.

Annexe B – Classement des risques liés à l’opinion de l’équipe de vérification

Les définitions suivantes sont utilisées pour classer l’opinion de l’équipe de vérification présentée dans ce rapport.

Bien contrôlé	Seules certaines faiblesses insignifiantes relatives aux objectifs de contrôle ou à la bonne gestion de l’activité vérifiée sont relevées.
Généralement acceptable	Les faiblesses relevées, prises individuellement ou collectivement, ne sont pas importantes ou des mécanismes compensatoires sont en place. Les objectifs de contrôle ou la bonne gestion de l’activité vérifiée ne sont pas compromis.
Nécessite une amélioration	Les faiblesses relevées, prises individuellement ou collectivement, sont importantes et peuvent compromettre les objectifs de contrôle ou la bonne gestion de l’activité vérifiée.

Annexe C – Recommandations et réponse de la direction

Recommandation issue de la vérification	Réponse de la direction	Calendrier d'achèvement
Recommandation 1 Il est recommandé que le sous-ministre adjoint, Secteur de la dirigeante principale des finances et des services ministériels, élabore un cadre de gouvernance officiel pour la cybersécurité qui comprend notamment : • les rôles et les responsabilités; • la formation obligatoire et les activités de sensibilisation.	**Réponse de la direction** La direction approuve en partie cette recommandation. **Cadre de gouvernance de la cybersécurité et rôles et responsabilités connexes** La Direction générale de la technologie de l'information, de la gestion de l'information, de l'administration et de la protection des renseignements personnels rendra officiel son cadre de gouvernance de la cybersécurité, y compris les rôles et les responsabilités. La gouvernance actuelle relève du Conseil consultatif sur le numérique, et c'est par l'entremise de ce dernier que nous établirons d'autres rapports de haut niveau. Nous documenterons également de façon officielle les principaux rôles et responsabilités en matière de cybersécurité qui ne sont pas suffisamment documentés dans les instruments de politique du Secrétariat du Conseil du Trésor (SCT). Ce cadre sera conforme à la *Politique sur la sécurité du gouvernement* et à la *Politique sur les services et le numérique* du SCT. **Formation et sensibilisation** Comme il a été mentionné, le Ministère a mis en œuvre une formation obligatoire pour les employés. Cette formation, qui est offerte par l'École de la fonction publique du Canada, sera gérée et régulièrement mise à jour par l'École en fonction des besoins du	Achèvement complet d'ici décembre 2026

	gouvernement du Canada. Le Ministère pourra ainsi s'assurer que la formation est impérative et à jour à l'avenir. En ce qui concerne la formation des employés, le Ministère n'établira pas de plan de formation normalisé pour les employés de la sécurité des technologies de l'information et laissera au gestionnaire de l'unité le soin de gérer la formation selon ses besoins et ses objectifs. Le choix de cette approche repose sur les facteurs suivants : 1.Une formation offerte à un petit groupe d'employés serait gérée plus efficacement par le gestionnaire qui est en contact direct avec ces employés. 2. Le contexte de la sécurité évolue rapidement et la formation doit pouvoir être modifiée en fonction des impératifs de sécurité actuels. Les employés ont des objectifs différents et la formation doit correspondre à leur rôle et à leurs besoins.	
<u>Recommandation 2</u> Il est recommandé que le sous-ministre adjoint du Secteur du dirigeant principal des finances et des services ministériels s'assure que le réseau d'ACC est efficacement protégé et surveillé en permanence contre les menaces potentielles :	**<u>Réponse de la direction</u>** La direction est d'accord avec cette recommandation. **Analyse de l'environnement et faisabilité de l'outil** L'équipe de sécurité de la TI examinera et documentera les procédures et les sources surveillées pour la sécurité du réseau d'ACC et des appareils	Achèvement complet d'ici mars 2027

• en élaborant et en mettant en œuvre des processus et des procédures visant à surveiller adéquatement le réseau d'ACC et les appareils connectés; • en explorant la possibilité d'intégrer un outil central de production de rapports; • en effectuant une analyse des services supplémentaires du CCC et en mettant en place ceux qui sont jugés avantageux pour ACC.	connectés afin d'assurer l'uniformité et la continuité des activités. Elle examinera également les sources pour s'assurer qu'il n'y a pas de chevauchement entre ACC et les partenaires de sécurité. En fonction de ces résultats, l'équipe déterminera les exigences à suivre et si un outil est nécessaire et faisable, et si c'est le cas, mettra en œuvre cet outil. **Évaluation des services de Mon cyberportail** L'équipe de sécurité de la TI évaluera les systèmes et les services offerts par l'entremise de Mon cyberportail. Si un service est jugé avantageux pour le Ministère et que des ressources internes suffisantes sont disponibles pour soutenir son utilisation, la Sécurité de la TI s'abonnera au service.	

Recommandation 3	**Réponse de la direction**	Achèvement complet d'ici mars 2026
Il est recommandé que le sous-ministre adjoint du Secteur du dirigeant principal des finances et des services ministériels prend des mesures pour atténuer les risques de cybersécurité : • en élaborant un plan d'action pour mettre en œuvre les recommandations existantes issues de l'exercice du PGEC avec un calendrier de mise en œuvre connexe; • en créant un plan pour mener des exercices supplémentaires sur le PGEC à intervalles réguliers avec un mécanisme pour assurer la mise en œuvre des recommandations qui en découlent en temps opportun.	La direction est partiellement d'accord avec cette recommandation. **Recommandations découlant du PGEC :** La Direction du cyber, de la gestion de l'information et des services de données mettra en œuvre les recommandations 1, 2 et 4. • Les recommandations 1 et 2 impliquent la création d'une matrice des rôles et des responsabilités qui indique les décideurs clés. • La recommandation 4 implique la réalisation d'un exercice du PGEC tous les deux ans. **Aucune autre mesure ne sera prise pour la recommandation suivante :** • La recommandation 3 est liée à la tenue à jour de la documentation pour le PGEC et le PCA, ce qui sera fait au moyen d'exercices menés tous les deux ans et de processus du PCA. • La recommandation 5 décrit la préparation de conseils sur les mesures de soutien aux clients pour lesquelles le Ministère demanderait des conseils et des directives au CCC et au SCT. Par conséquent, nous n'élaborerions pas nos propres procédures et conseils pour ce point. • La recommandation 6 relative à la propension au risque en général continuera de faire l'objet d'un examen minutieux et d'un taux de réponse élevé, comme l'indiquent le cadre ministériel de gestion des	

	risques et la position actuelle du gouvernement du Canada sur la cybersécurité. Les éléments de risque feront l'objet de discussions dans le cadre de mises à jour sur la gouvernance ainsi que de séances d'information situationnelles qui auront lieu dans le cadre de la nouvelle gouvernance et, par conséquent, nous ne participerons pas à un exercice distinct. • La recommandation 7 concernant les modèles de communication n'aurait pas suffisamment d'avantages, car les communications dépendront grandement du scénario et de nombreuses situations uniques. Les communications seront guidées par le CCC et le SCT pour les scénarios plus complexes, et pour quelque chose de peu fréquent, il en résultera un lourd fardeau de tenir le matériel constamment à jour pour un avantage minime. • La recommandation 8 concernant les menaces internes par rapport aux menaces externes est prise en compte dans toutes les situations et fait partie des connaissances et des pratiques courantes en matière de sécurité. • La recommandation 9 relative à la saisie des dossiers d'incidents est décrite à plusieurs reprises dans les modèles du PGEC et est intégrée au processus. Il n'y a pas beaucoup d'avantages à offrir une formation spécifique aux personnes sur la saisie de notes, car il peut s'agir de plusieurs personnes et il s'agit	

	généralement d'une pratique courante. La recommandation 10 est une considération notée concernant le confinement par rapport à l'élimination et ferait partie des considérations normalisées d'un analyste de la cybersécurité. Aucune mesure supplémentaire ne serait nécessaire.	