Audit de la gouvernance de la cybersécurité et de la sécurité de la TI

Table des matières

Contexte

La cybersécurité est une responsabilité partagée entre Services partagés Canada (SPC), le Centre canadien pour la cybersécurité (CCC), le Centre de la sécurité des télécommunications (CST), le Secrétariat du Conseil du Trésor du Canada (SCT) et les organisations partenaires. Parmi ces organisations, SPC, le CCC et le SCT sont connus collectivement sous le nom de Comité tripartite sur la sécurité de la TI (Comité tripartite) du gouvernement du Canada (GC). Les organisations du Comité tripartite assument des responsabilités particulières et fournissent des services précis à l'échelle du gouvernement, y compris pour le mandat plus restreint de la cyberdéfense.

En tant que fournisseur de services de TI du GC, SPC continue de se concentrer sur le renforcement de la cybersécurité et sur la défense de l'infrastructure de TI du GC contre les attaques sur les réseaux, les logiciels malveillants et les autres cybermenaces. Les cyberattaques sont de plus en plus fréquentes, et les auteurs de menaces utilisent des technologies sophistiquées, telles que l'intelligence artificielle (IA), pour découvrir et exploiter les vulnérabilités des systèmes du GC. À mesure que le niveau de sophistication des cybermenaces augmente, SPC doit évoluer pour renforcer les capacités de cybersécurité nécessaires pour gérer le contexte des cybermenaces.

SPC est assujetti à la Politique sur les services et le numérique du Conseil du Trésor (CT) et à la Politique sur la sécurité du gouvernement du CT, qui définissent les exigences en matière de cybersécurité et de sécurité de la TI pour les ministères et les organismes. SPC a défini plus précisément les rôles et les responsabilités en matière de cybersécurité et de sécurité de la TI dans la Politique sur la sécurité ministérielle, la Directive sur la gestion de la sécurité ministérielle et la Directive sur la gestion de la sécurité pour les services intégrés de SPC.

L’approche de SPC en matière de cybersécurité et de sécurité de la TI comporte deux volets, comme c’est défini dans ses instruments de politique :

- Services de sécurité intégrés – services de cybersécurité et de sécurité de la TI fournis par SPC aux ministères du GC;
- Services de sécurité ministériels – services internes qui créent un environnement sûr et sécurisé assurant la protection des personnes sur le lieu de travail, ainsi que des renseignements et actifs sous le contrôle du Ministère, et permettant la prestation continue des programmes et services ministériels [1].

Pour renforcer les services de sécurité intégrés, SPC, sous la direction du dirigeant principal de la technologie (DPT), élaborera un programme de cybersécurité en collaboration avec le sous-ministre adjoint principal de la Direction générale des services de réseaux et de sécurité (DGSRS). Le programme de cybersécurité renforcera la gouvernance et les capacités en matière de cybersécurité, et fera constamment évoluer le niveau de sécurité du GC de façon à améliorer la réponse aux besoins opérationnels et la gestion des nouvelles menaces. Au moment de l’audit, le programme de cybersécurité n’avait pas encore été mis en place. La responsabilité du programme et les responsabilités connexes en matière de cybersécurité ont toutefois été déléguées au DPT depuis 2022.

Objectif, portée et méthode de l’audit

Objectif

L’objectif du présent audit était d’apporter une assurance concernant les éléments suivants : l’efficacité de la structure de gouvernance; la définition, la documentation, la communication et la bonne compréhension des rôles

et des responsabilités en matière de cybersécurité et de sécurité de la TI dans l'ensemble du Ministère; l'intégration de la cybersécurité et de la sécurité de la TI dans les principaux secteurs d'activité, y compris la gestion des services, l'architecture d'entreprise et les opérations infonuagiques.

Portée

L'audit a porté à la fois sur les services ministériels et sur les services intégrés, et visait ce qui suit :

- le cadre de gouvernance de la cybersécurité et de la sécurité de la TI de SPC;
- l'efficacité de la prise de décision;
- la politique et l'orientation;
- les responsabilités, les rôles et les obligations en matière de gestion des fonctions de cybersécurité et de sécurité de la TI de SPC;
- la planification intégrée de la cybersécurité et de la sécurité de la TI;
- la gestion des risques liés à la cybersécurité et à la sécurité de la TI;
- la supervision, y compris la surveillance et l'établissement de rapports.

L'audit a visé la période du 1er janvier 2022 au 30 septembre 2023.

La portée excluait les fonctions opérationnelles liées à la cybersécurité et à la sécurité de la TI, telles que la gestion des correctifs, la gestion des vulnérabilités, l'évaluation et autorisation de sécurité (EAS) ainsi que la planification de la continuité des activités de TI, étant donné que ces domaines ont été visés par des audits récents.

Méthode

L'audit a été réalisé grâce aux moyens suivants :

- entrevues menées avec la haute direction et des membres du personnel opérationnel ayant des rôles et des responsabilités en matière de cybersécurité et de sécurité de la TI;
- entrevues avec des membres sélectionnés des comités et des conseils responsables de la cybersécurité et de la sécurité de la TI;
- examen de la documentation, y compris les comptes rendus des décisions, les ordres du jour et les documents de présentation de chacun des comités et des conseils responsables de la cybersécurité et de la sécurité de la TI;
- examen des pratiques de gestion des risques liés à la cybersécurité et à la sécurité de la TI;
- détermination des contrôles principaux.

Énoncé de conformité

Le présent audit a été réalisé en conformité avec le *Cadre de référence international des pratiques professionnelles* de l'Institute of Internal Auditors et avec la *Politique sur la vérification interne* du Conseil du Trésor du Canada, comme en témoignent les résultats du programme d'amélioration et d'assurance de la qualité du Bureau de la vérification et de l'évaluation.

Constatations

Les constatations découlant de l'audit ont été préparées au moyen d'un processus de comparaison des critères (le bon état) avec la condition (l'état actuel). Le cas échéant, des recommandations ont été formulées en ce qui concerne les conditions qui ont été indiquées comme des domaines à améliorer. Une conclusion globale de l'audit a également été formulée par rapport à l'objectif de l'audit.

Les constatations, les recommandations et les conclusions de cette mission d'audit interne ont été communiquées à la direction et au Comité ministériel d'audit de SPC.

Réponse de la direction

La direction est d'accord avec les constatations et a accepté les recommandations du rapport d'audit. Le cas échéant, la Direction générale du dirigeant principal de la technologie, la Direction générale de l'approvisionnement en TI pour l'entreprise et des services ministériels, la Direction générale des services de réseaux et de sécurité ainsi que la Direction générale de la stratégie et de la mobilisation ont élaboré des plans d'action pour donner suite aux constatations et aux recommandations. Le Bureau de la vérification et de l'évaluation surveillera la mise en œuvre de ces plans.

Secteurs d'intérêt et critères

Secteur d'intérêt 1 : Gouvernance

1.1 SPC dispose d'un régime de surveillance pour gérer les risques et les enjeux liés à la cybersécurité et à la sécurité de la TI :

a. SPC a défini la structure des organes de gouvernance afin de gérer efficacement les risques et les enjeux liés à la cybersécurité;
b. SPC a intégré la gouvernance de la cybersécurité et de la sécurité de la TI dans la gestion des principales activités d'entreprise (infonuagique, gestion des services, gestion des projets et architecture d'entreprise);
c. la haute direction dispose de renseignements suffisants pour prendre, en temps opportun, des décisions en matière de cybersécurité et de

sécurité de la TI.

1.2 SPC a élaboré, documenté et communiqué un instrument politique qui comprend la cybersécurité et la sécurité de la TI :

a. les instruments de politique sont à jour et incluent les activités de cybersécurité et de sécurité de la TI ministérielles et d'entreprise;
b. les instruments de politique sont conformes au cadre de politique du GC.

1.3 Les rôles et les responsabilités de SPC en matière de cybersécurité et de sécurité de la TI sont définis, documentés, communiqués et tenus à jour comme il convient :

a. les rôles et les responsabilités entre SPC et ses partenaires (Comité tripartite, clients) pour l'entreprise sont clairs, documentés et communiqués;
b. les rôles et les responsabilités de SPC en matière de cybersécurité et de sécurité de la TI sont harmonisés dans tous les domaines fonctionnels (ministériels et d'entreprise);
c. SPC a désigné l'agent responsable de la fonction de la cybersécurité conformément à la Politique sur les services et le numérique du CT, et a défini la manière dont ce rôle est lié au reste du cadre de politique ministériel;
d. les responsabilités et les obligations en matière de gestion des incidents et des événements liés à la cybersécurité et à la sécurité de la TI sont définis, coordonnés, documentés, communiqués et compris par tous les intervenants qui jouent un rôle dans la cybersécurité et la sécurité de la TI.

1.4 SPC a élaboré un plan de cybersécurité ministériel qui a été approuvé par la haute direction :

a. le plan porte sur une stratégie de cybersécurité, un programme de cybersécurité, des feuilles de route et des plans d'action;
b. la planification de la cybersécurité a été intégrée dans d'autres domaines de planification (c.-à-d. infrastructure, données, services, approvisionnement et gestion de la capacité).

Secteur d'intérêt 2 : Gestion des risques

2.1 SPC a mis en œuvre un processus de gestion des risques qui reflète avec précision les risques liés à la cybersécurité et à la sécurité de la TI, y compris l'établissement de niveaux de tolérance au risque nécessaires pour déterminer les priorités en vue de la prise de décision.

Secteur d'intérêt 3 : Surveillance et établissement de rapports

3.1 SPC a mis en place des mécanismes appropriés de surveillance et d'établissement de rapports qui comprennent ce qui suit :

a. le respect des politiques de SPC et du GC;
b. des paramètres clés concernant la cybersécurité et la sécurité de la TI qui font l'objet d'une surveillance et de rapports périodiques présentés à la haute direction;
c. un ensemble normalisé d'éléments déclencheurs et d'outils qui ont été mis en œuvre pour garantir l'exactitude et l'exhaustivité des rapports.

Note de bas de page

1 Définition extraite de la Politique sur la sécurité ministérielle de SPC (annexe A).

Date de modification :

2025-07-08