Services publics et Approvisionnement Canada | Public Services and Procurement Canada

Canada

Au service du GOUVERNEMENT, au service des CANADIENS.

SUIVI DE L'AUDIT DE LA SÉCURITÉ INFORMATIQUE – Résumé

Bureau du dirigeant principal d'audit, évaluation et gestion du risque

Introduction

1. Cet engagement figurait dans le Plan d’audit fondé sur les risques de 2020 à 2021 de Services publics et Approvisionnement Canada (SPAC).
2. SPAC appuie les opérations quotidiennes du gouvernement du Canada en tant que fournisseur de services communs pour les ministères et organismes fédéraux. Plusieurs de ces services reposent sur la technologie de l’information (TI) qui, dans un environnement technologique global en rapide évolution, constitue de plus en plus une source de risques pour la confidentialité, l’intégrité et la disponibilité de l’information et des systèmes dont dépendent les opérations du Ministère.
3. Comme tous les ministères du gouvernement fédéral, SPAC est tenu de respecter les exigences de sécurité de base du Secrétariat du Conseil du Trésor, telles qu’énumérées dans la Politique sur la sécurité du gouvernement et dans la Directive sur la gestion de la sécurité connexe, entrées en vigueur le 1er juillet 2019. L’objectif de cette politique est d’encadrer la gestion efficace des mesures de sécurité gouvernementales pour assurer la fiabilité des programmes et services du gouvernement du Canada, protéger les renseignements, les personnes et les biens, et de maintenir la confiance de la population canadienne, des partenaires, des organismes de surveillance et des autres intervenants à l’égard de la gestion de la sécurité au sein du gouvernement du Canada. La politique oblige tous les ministères à établir un programme de sécurité de la coordination et de la gestion des activités de sécurité ministérielle, divisés en huit domaines de contrôle de la sécurité, y compris la cybersécurité (sécurité de la TI).

Objectif de l’audit

4. L’objectif de cet engagement était de confirmer que des mécanismes adéquats sont en place pour gérer les risques liés à la cybersécurité. Il fallait donc vérifier que les mesures de contrôle de gestion du programme ministériel de cybersécurité ont été adoptées et qu’elles fonctionnent comme prévu, que les applications opérationnelles de SPAC sont corrigées rapidement, et que SPAC gère efficacement les risques entourant la cybersécurité dans le cadre de ses opérations pendant la pandémie (COVID-19).

Portée de l’audit

5. L’audit s’est déroulé du 1er août 2019 au 30 novembre 2020. Les renseignements pertinents obtenus après notre phase d’examen ont été pris en compte.
6. L’audit s’est penché sur les procédés et les contrôles en place en matière de cybersécurité pour les principaux secteurs de contrôle suivants :
    - Gestion du programme de cybersécurité;
    - Gestion des correctifs et des vulnérabilités;

- Gestion des risques émergents en matière de cybersécurité en raison de la COVID-19.

7. L’audit n’a pas pris en compte les secteurs de l’audit de la sécurité de la TI désignés comme étant terminés en octobre 2019.
8. L’audit ne portait pas sur les systèmes des RH et de la paye.

Observations

9. Les observations découlant de l’audit ont été élaborés au moyen d’un processus de comparaison des critères (le bon état) avec la condition (l’état actuel). Les observations suivantes peuvent indiquer un rendement satisfaisant, quand la condition remplit les critères, ou elles peuvent noter des points à améliorer, quand il y a une différence entre la condition et les critères. Le cas échéant, des recommandations ont été formulées en vue des conditions qui ont été notées comme des domaines à améliorer. Une conclusion générale de l’audit a également été formulée par rapport à l’objectif de l’audit.
10. Les observations, recommandations, conclusion de cette mission d’audit interne ont été signalés à la haute direction et le Comité ministériel d’audit de SPAC.

Réponse de la direction

11. La direction est d'accord avec les constatations et accepte les recommandations de cet audit interne. Le cas échéant, la Direction générale des services numérique et la Direction générale de la surveillance ont élaboré des plans d'action pour donner suite aux constatations et aux recommandations, dont la mise en œuvre sera surveillée par le Bureau du dirigeant principal de l’audit, évaluation et gestion du risque.
12. SPAC s’engage à veiller à ce que les activités clé de contrôle visant à atténuer les risques de sécurité informatique soient conçues, mises en œuvre et fonctionnant comme prévu.

Approche de l’audit

13. L'audit interne a été mené conformément aux *Normes internationales pour la pratique professionnelle de l'audit interne*, comme le confirment les résultats du programme d'assurance et d'amélioration de la qualité.