Secrétariat du Conseil du Trésor du Canada
Treasury Board of Canada Secretariat
Canada

Audit coordonné de la sécurité de la technologie de l'information (avec Services partagés Canada)

Publié : le 2018-01-05

Publié par le Secrétariat du Conseil du Trésor du Canada
90 rue Elgin, Ottawa, Ontario, K1A 0R5, Canada

No de catalogue BT66-80/2018F-PDF
ISBN : 978-0-660-43956-3

Ce document est disponible sur Canada.ca, le site Web du gouvernement du Canada.

Ce document est disponible en médias substituts sur demande.

Nota : Pour ne pas alourdir le texte français, le masculin est utilisé
pour désigner tant les hommes que les femmes.

Also available in English under the title: Coordinated Audit of Information Technology Security (with Shared Services Canada)

Audit coordonné de la sécurité de la technologie de l’information (avec Services partagés Canada)

Note aux lecteurs :

Ce rapport contient des renseignements qui ont été retranchés conformément à la Loi sur l'accès à l'information.

Table des matières

Énoncé de conformité

Le Bureau de la vérification interne et de l'évaluation a terminé l'audit coordonné de la sécurité de la technologie de l'information (TI (technologies de l'information)). Cet audit est conforme aux Normes relatives à la vérification interne au sein du gouvernement du Canada, comme en témoignent les résultats du programme d'assurance de la qualité et d'amélioration du Bureau.

Sommaire

Contexte

Cet audit faisait partie du plan approuvé d'audit axé sur le risque de 2014 à 2017 du Secrétariat du Conseil du Trésor du Canada. Il a été réalisé dans le but de donner une assurance supplémentaire, qui était hors de la portée d'un récent audit horizontal de la sécurité des TI (technologies de l'information) dans les grands et les petits ministères, effectué par le Bureau du contrôleur général du Canada.

Le gouvernement du Canada a adopté une approche axée sur la « défense en profondeur [1] » relativement à la gestion de la sécurité de la TI (technologies de l'information) afin de protéger ses données et ses systèmes. Cette approche est fondée sur plusieurs couches de mesures de sécurité visant à prévenir et à réduire l'exploitation possible des vulnérabilités.

Services partagés Canada (SPC) et les autres principaux organismes chargés de la sécurité (la Direction du dirigeant principal de l'information du gouvernement du Canada, le Centre de la sécurité des télécommunications Canada et Sécurité publique Canada) coordonnent les activités de sécurité de la TI (technologies de l'information) dans le but de protéger le périmètre de réseau du gouvernement contre les menaces externes. Cette coordination comprend l'application des

mesures de sécurité nécessaires ainsi que la surveillance des activités sur le réseau du gouvernement. Le réseau ministériel du Secrétariat se situe à l'arrière du périmètre de réseau du gouvernement.

Dans le cadre de cet audit, on a examiné le caractère adéquat des contrôles de sécurité de la TI (technologies de l'information) qui étaient en place pour protéger le réseau et l'infrastructure du Secrétariat. Compte tenu des responsabilités réparties en matière de contrôles de sécurité de la TI (technologies de l'information) et de la coordination nécessaire avec Services partagés Canada, les groupes de la vérification interne du Secrétariat et de Services partagés Canada ont adopté une approche d'audit coordonnée afin d'offrir une plus vaste assurance.

Objectif et portée

L'audit avait pour objectif d'évaluer le caractère adéquat et l'efficacité des contrôles internes à l'égard de la gestion de la sécurité de la TI (technologies de l'information) ministérielle, y compris la conformité avec les politiques et les normes applicables.

La portée de l'audit était centrée sur les services et les processus opérationnels ayant la plus grande incidence possible sur la sécurité de la TI (technologies de l'information) au Secrétariat et pour lesquels une collaboration ou une coordination entre Services partagés Canada et le Secrétariat s'impose.

Les processus se rapportant au développement de logiciels, à l'accès aux applications opérationnelles et au réseau secret du gouvernement du Canada ont été exclus de la portée de l'audit.

Les procédures d'audit ont été entamées en septembre 2015 dans le but de tirer parti du travail accompli dans le cadre de l'audit horizontal de la sécurité des TI (technologies de l'information) effectué par le Bureau du contrôleur général du Canada. La phase d'examen a été terminée en août 2016.

Résultats de l'audit

L'audit était centré sur quatre aspects importants de la gestion de la TI (technologies de l'information) au Secrétariat : la gestion des accès des utilisateurs, la gestion des incidents, la gestion des changements et la gestion des risques relatifs à la sécurité de l'information. L'équipe d'audit a conclu, avec un niveau d'assurance raisonnable, que, les contrôles relatifs à la gestion de la sécurité de la TI (technologies de l'information) ministérielle étaient en grande partie efficaces et conçus adéquatement.

Même si les résultats ont été positifs dans l'ensemble pour les secteurs à l'égard desquels le Secrétariat est autorisé à agir, l'audit a relevé des contrôles qui devraient être renforcés [L'information a été retranchée] afin d'atténuer pleinement les risques pour les ramener à un niveau acceptable. Ces contrôles se rapportent aux contrôles internes du Secrétariat de même qu'à la nécessité d'améliorer la coordination et la collaboration entre le Secrétariat et Services partagés Canada.

Plus précisément, les points suivants s'appliquent.

- Des processus sont en place pour cerner et classifier correctement les serveurs où des renseignements sensibles sont stockés. De plus, les utilisateurs ont généralement les droits d'accès appropriés pour exécuter leurs fonctions. [L'information a été retranchée]
- Des processus ministériels sont en place afin de surveiller les activités de réseau liées aux incidents de sécurité. [L'information a été retranchée]
- Les propriétaires de renseignements et les propriétaires de systèmes d'information ont des rôles et des responsabilités déterminants au regard de certains aspects de la sécurité de la TI (technologies de l'information). [L'information a été retranchée]
- Il existe des possibilités d'établir une approche fondée sur le risque afin d'assurer en temps utile la transformation des services du Secrétariat en vue du stade final de Services partagés Canada [L'information a été retranchée]

[L'information a été retranchée] recommandations ont été formulées à l'appui de l'amélioration des contrôles internes à l'égard de la gestion de la sécurité de la TI (technologies de l'information) ministérielle au Secrétariat.

Réponse de la direction

Le Secrétariat a élaboré une réponse et un plan d'action de la direction, qui sont présentés à l'annexe A.

[L'information a été retranchée]

1. Introduction

Le Secrétariat du Conseil du Trésor du Canada est l'organe administratif du Conseil du Trésor. Le Secrétariat aide le Conseil du Trésor à établir les règles régissant la gestion des personnes, des fonds publics et des biens du gouvernement, à gérer les plans de dépenses du gouvernement et à assurer l'intendance des fonds publics, à envisager et à recommander des modifications réglementaires ayant une incidence sur la santé et la sécurité des Canadiens, l'économie et l'environnement, et à déterminer les conditions d'emploi de l'administration publique centrale [2]. Cette aide est offerte par plus de 1 700 employés [3] qui accèdent aux renseignements sur le réseau du Secrétariat selon les principes de sécurité de base du « privilège minimal », du « besoin d'avoir » et du « besoin de connaître ».

La création de Services partagés Canada en 2011 est venue rassembler des personnes, des ressources technologiques et des biens de 43 ministères et organismes dans le but d'accroître l'efficience, la fiabilité et la sécurité de l'infrastructure de la TI (technologies de l'information) du gouvernement. À compter du 15 novembre 2011, Services partagés Canada a assumé la responsabilité des services de courriel, de centre de données et de réseau pour le Secrétariat (l'infrastructure de la TI (technologies de l'information)). Le maintien de la posture de sécurité de la TI (technologies de l'information) du Secrétariat est devenu une responsabilité partagée entre le Secrétariat et Services partagés Canada.

Une approche d'audit coordonnée a été adoptée afin d'évaluer la posture de sécurité de la TI (technologies de l'information) pour les secteurs à responsabilité partagée. L'approche coordonnée permettait à chaque ministère d'examiner les activités de sécurité de la TI (technologies de l'information) réalisées sous son ministère respectif et sa responsabilité respective, ainsi que d'évaluer les activités à chaque

étape du processus sans être ralenti par les limites ministérielles. Les résultats ont été partagés entre les fonctions de vérification interne des deux ministères, mais chacun d'eux présentera les résultats concernant sa propre organisation.

1.1 Organizations

Le gouvernement du Canada a adopté une approche axée sur la « défense en profondeur [4] » relativement à la gestion de la sécurité de la TI (technologies de l'information) afin de protéger ses données et ses systèmes. Cette approche est fondée sur plusieurs couches de mesures de sécurité visant à prévenir et à réduire l'exploitation possible des vulnérabilités.

Services partagés Canada a le mandat de fournir des services de centre de données, de réseau et de courriel à 43 ministères et organismes fédéraux (les organisations partenaires). Services partagés Canada, le Centre de la sécurité des télécommunications Canada et Sécurité publique Canada se partagent la responsabilité de la cybersécurité et de la sécurité de la TI (technologies de l'information). Une surveillance est assurée par le Secrétariat et un soutien est offert par la Direction du dirigeant principal de l'information. Ces organisations coordonnent les activités de sécurité de la TI (technologies de l'information) afin de protéger le périmètre de réseau du gouvernement contre les menaces externes. Entre autres, elles appliquent les mesures de sécurité nécessaires et surveillent les activités sur le réseau du gouvernement. Le réseau ministériel du Secrétariat se situe à l'arrière du périmètre de réseau du gouvernement.

Dans le cadre de cet audit, on a examiné le caractère adéquat des contrôles de sécurité de la TI (technologies de l'information) qui étaient en place pour protéger le réseau et l'infrastructure du Secrétariat.

Le maintien d'une robuste posture de sécurité de la TI (technologies de l'information) interne nécessite une vigilance continue de la part du Secteur des services ministériels du Secrétariat, avec la collaboration de Services partagés Canada et une coordination avec ce dernier.

L'audit était centré sur les activités de la Direction de la gestion de l'information et de la technologie du Secteur des services ministériels du Secrétariat.

Compte tenu des responsabilités réparties en matière de contrôles de sécurité de la TI (technologies de l'information) et de la coordination nécessaire avec Services partagés Canada, les groupes de la vérification interne du Secrétariat et de Services partagés Canada ont adopté une approche d'audit coordonnée afin d'offrir une plus vaste assurance.

2. Détails de l'audit

2.1 Autorisation

L'audit coordonné de la sécurité de la technologie de l'information fait partie du plan approuvé d'audit axé sur le risque pour 2014 à 2017 du Secrétariat.

2.2 Objectifs et portée

La portée de l'audit était centrée sur les services et les processus opérationnels ayant la plus grande incidence possible sur la sécurité de la TI (technologies de l'information) au Secrétariat et pour lesquels une collaboration ou une coordination entre Services partagés Canada et le Secrétariat s'impose. Plus précisément, il s'agit de ce qui suit :

- la gestion des accès des utilisateurs;
- la gestion des incidents de sécurité de la TI (technologies de l'information);
- la gestion des changements ayant une incidence possible sur la sécurité de la TI (technologies de l'information);
- la gestion des risques pour la sécurité de la TI (technologies de l'information).

Les procédures d'audit ont été appliquées aux activités réalisées entre le 1er avril 2014 et juin 2015. Des éléments de preuve produits en dehors de cette période ont également été pris en considération. Les activités de la sécurité de la TI (technologies de l'information) réalisées par Services partagés Canada au nom du

Secrétariat ont été examinées et évaluées par le Bureau de la vérification et de l'évaluation de Services partagés Canada, et elles sont présentées dans un rapport distinct.

L'audit a été lancé en février 2015. Les procédures d'audit ont été amorcées en septembre 2015 afin de tirer parti du travail accompli dans le cadre de l'audit horizontal de la sécurité des TI (technologies de l'information) effectué par le Bureau du contrôleur général.

2.3 Éléments exclus de la portée

L'audit a exclu les éléments suivants.

- **Développement de logiciels :** Des activités limitées de développement de logiciels sont réalisées par Services partagés Canada pour les systèmes du Secrétariat; par conséquent, on a estimé que ces activités présentent un risque faible, et elles ont été exclues de la portée de cet audit.
- **Accès aux applications opérationnelles :** L'accès aux applications opérationnelles, y compris les logiciels non standards, n'a pas été inclus dans la portée de l'audit en raison de l'absence de la coordination nécessaire entre Services partagés Canada et le Secrétariat au cours de ce processus.
- **Réseau secret du gouvernement du Canada :** Le réseau secret du gouvernement du Canada a été exclu de cet audit [L'information a été retranchée]. Le Bureau du contrôleur général du Canada a désigné la gestion des renseignements classifiés comme un secteur de risque à étudier à l'avenir [5] au cours d'un audit distinct.

2.4 Approche et méthode

L'approche et la méthode de l'audit étaient fondées sur les risques et étaient conformes aux Normes relatives à la vérification interne au sein du gouvernement du Canada. Ces normes exigent que l'audit soit planifié et mené de façon à donner l'assurance raisonnable que les objectifs de l'audit sont atteints.

L’audit comprenait divers essais et diverses procédures que l’on considère comme nécessaires afin de donner une telle assurance, y compris les éléments suivants :

- des entrevues avec des employés clés de Services partagés Canada et du Secrétariat;
- l’examen de documents;
- des revues générales;
- des essais des contrôles;
- des essais substantiels;
- une analyse de données.

2.5 Champs d’enquête

L’audit comprenait quatre champs d’enquête.

- **Gestion des accès des utilisateurs :** Les renseignements du Secrétariat sont protégés contre les accès non autorisés afin de maintenir un niveau de risque pour la sécurité de l’information qui est acceptable au Secrétariat, conformément aux instruments de politique et aux procédures de sécurité applicables. Des rôles de sécurité de l’information et des privilèges d’accès à l’information sont établis et tenus à jour, et une surveillance de la sécurité est assurée.
- **Gestion des incidents de sécurité de la TI (technologies de l’information) :** Une intervention efficace et rapide face à d’éventuels incidents de sécurité de l’information. Les incidents sont consignés, soumis à une enquête, analysés, transmis aux échelons supérieurs et résolus.
- **Gestion des changements ayant une incidence possible sur la sécurité de la TI (technologies de l’information) :** Les changements touchant les systèmes de la TI (technologies de l’information) qui ont une incidence sur la sécurité sont gérés d’une façon contrôlée. De tels changements visent entre autres les normes et les procédures, l’évaluation des répercussions sur la sécurité, l’établissement des priorités, l’autorisation, les changements d’urgence, le suivi, la production de rapports, la fermeture et la documentation.

- **Gestion des risques pour la sécurité de la TI (technologies de l'information) :** L'exposition aux risques pour la sécurité de la TI (technologies de l'information) est continuellement évaluée et réduite pour être conforme aux niveaux de tolérance établis par la direction en collaboration avec Services partagés Canada.

Les critères d'audit ont été tirés de Objectifs de contrôle de l'Information et des Technologies Associées, version 5.0 (COBIT 5) et de la norme de gestion de la sécurité de l'information 27001 de l'ISO/IEC.

Les critères d'audit qui ont servi à évaluer chaque champ d'enquête sont présentés à l'annexe B.

3. Résultats de l'audit

Les résultats de l'audit sont présentés par champ d'enquête.

[L'information a été retranchée]

Conclusion globale

L'équipe d'audit a conclu, avec un niveau d'assurance raisonnable, que, les contrôles relatifs à la gestion de la sécurité de la TI (technologies de l'information) ministérielle étaient en grande partie efficaces et conçus adéquatement.

Même si les résultats ont été positifs dans l'ensemble pour les secteurs à l'égard desquels le Secrétariat est autorisé à agir, l'audit a relevé des contrôles qui devraient être renforcés dans les quatre secteurs de la portée de l'audit afin d'atténuer pleinement les risques pour les ramener à un niveau acceptable. Ces contrôles se rapportent aux contrôles internes du Secrétariat de même qu'à la nécessité d'améliorer la coordination et la collaboration entre le Secrétariat et Services partagés Canada.

[L'information a été retranchée] recommandations ont été formulées à l'appui de l'amélioration des contrôles internes à l'égard de la gestion de la sécurité de la TI (technologies de l'information) ministérielle au Secrétariat. Elles sont présentées à

l’annexe A, conjointement avec les mesures de la direction visant à y donner suite.

Annexe A : Réponse de la direction

[L’information a été retranchée]

Annexe B : Critères d’audit

[L’information a été retranchée]

Notes en bas de page

1 Le Plan stratégique de la technologie de l’information du gouvernement du Canada 2016-2020, La sécurité de la TI (technologies de l’information)

2 Rapport ministériel sur le rendement du Secrétariat du Conseil du Trésor du Canada pour 2015 2016

3 Effectif de la fonction publique fédérale par ministère : Secrétariat du Conseil du Trésor du Canada

4 Le Plan stratégique de la technologie de l’information du gouvernement du Canada 2016-2020, « La sécurité de la TI (technologies de l’information) »

5 Bureau du contrôleur général du Canada, Plan d’audit axé sur le risque pour 2016 à 2019, annexe H : Autres secteurs de risque cernés aux fins de considérations futures

---

Date de modification :
2017-10-18