Aboriginal Affairs and Northern Development Canada | Affaires autochtones et Développement du Nord Canada

Affaires autochtones et Développement du Nord Canada

Résumé du rapport de vérification interne

Vérification de la sécurité des technologies de l'information

Préparé par la

Direction générale des services de vérification et d'assurance

Avril 2015

TABLE DES MATIÈRES

Acronymes

AADNC	Affaires autochtones et Développement du Nord Canada
ASM	Agent de sécurité du ministère
CSTI	Coordonnateur de la sécurité des technologies de l'information
GSTI	Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information
PSM	Plan de sécurité ministérielle
TI	Technologies de l'information

Contexte

En tant que ministère du gouvernement fédéral, Affaires autochtones et Développement du Nord Canada (AADNC) est gouverné par la *Politique sur la sécurité du gouvernement* du Secrétariat du Conseil du Trésor du Canada (SCT). La sécurité du gouvernement, selon cette politique générale, fait référence à l'assurance que l'information, les biens et les services ne sont pas compromis et que les personnes sont protégées contre la violence en milieu de travail. En ce qui concerne la sécurité de l'information et des technologies de l'information (TI), il y a la *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information* (GSTI) du Conseil du Trésor, qui définit les exigences sécuritaires de base auxquelles les ministères et les organismes fédéraux doivent satisfaire pour assurer la sécurité de l'information et des biens de technologie de l'information placés sous leur contrôle.

Selon la GSTI, la sécurité des TI se définit comme étant les « mesures de sauvegarde visant à préserver la confidentialité, l'intégrité, la disponibilité, l'utilisation prévue et la valeur des renseignements conservés, traités ou transmis par voie électronique », et, aux fins de la norme, « les mesures de protection appliquées aux biens utilisés pour recueillir, traiter, recevoir, afficher, transmettre, reconfigurer, numériser, entreposer ou détruire l'information par voie électronique ».

Un programme de sécurité efficace réunit les outils et les technologies afin de protéger l'information et les systèmes, et assure la coordination d'une variété d'intervenants. À AADNC, les deux postes essentiels chargés de la sécurité des TI sont l'*agent de sécurité du ministère* (ASM), un directeur de la Sûreté et de la santé et sécurité au travail, de la Direction générale des services de ressources humaines et du milieu du travail, et le *coordonnateur de la sécurité des technologies de l'information* (CSTI), un gestionnaire de la sécurité des TI, de la Direction générale de la gestion de l'information dirigée par le dirigeant principal de l'information. Le CSTI relève, sur le plan fonctionnel, de l'ASM en ce qui a trait aux questions relatives à la sécurité.

En 2011, Services partagés Canada a été mis sur pied et chargé de la prestation de certains services des TI, ainsi que de la sécurité connexe, notamment des courriels, des centres de données (matériel informatique et logiciels d'exploitation connexes), des réseaux de télécommunications et des aspects liés à la cybersécurité, qui étaient anciennement fournis par AADNC.

Les risques associés à l'utilisation des TI évoluent au fur et à mesure que les technologies sont de plus en plus interdépendantes. Le fait qu'AADNC compte sur les TI pour traiter, stocker et transmettre l'information à l'appui de l'exécution continue de programmes, combiné à la nécessité du Ministère de protéger cette information, met en lumière le besoin de mettre en pratique des contrôles et des pratiques de sécurité rigoureuses en matière de TI.

Cette vérification a été ajoutée au plan de vérification axé sur les risques de 2014-2015 à 2016-2017 du Ministère, à la demande de la sous-ministre d'AADNC.

Objectif de la vérification

L'objectif de la vérification était de déterminer la pertinence et l'efficacité de ce qui suit :

- le cadre de gouvernance en place concernant la sécurité des TI pour protéger la sécurité de l'information ministérielle ainsi que pour aider à assurer la conformité à la *Politique sur la sécurité du gouvernement* et à la *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information*;
- les cadres de contrôle sélectionnés en place pour atténuer les risques liés à la sécurité des TI.

Portée de la vérification

La portée comprend un examen de la gouvernance, de la gestion du risque et des principaux contrôles de sécurité des TI conçus pour protéger la sécurité de l'information et les actifs en matière d'information, ainsi que pour aider à assurer la conformité à la *Politique sur la sécurité du gouvernement* et à la *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information*.

Outre le cadre de gouvernance visant tous les aspects de la sécurité des TI, des tests précis ont été menés sur les contrôles de sécurité des TI pour un éventail d'applications et de dossiers de réseau, ainsi que sur les contrôles mis en place pour protéger les ordinateurs de bureau, les ordinateurs portables et les supports amovibles.

Plus précisément, le travail de vérification comportait ce qui suit.

- Un examen des processus liés à la gouvernance de la sécurité des TI et à la gestion du risque en place visant à gérer le programme de sécurité des TI au Ministère. Ce volet portait sur le cadre stratégique de sécurité des TI; la gouvernance, les rôles et les responsabilités associés à la sécurité des TI; la planification de la sécurité des TI et la gestion du risque; la planification des ressources humaines; le respect des exigences du gouvernement fédéral.
- Un examen des contrôles pour un éventail de domaines où les données sont stockées électroniquement au sein du Ministère, notamment dans les applications et, si des données sont téléchargées, sur des ordinateurs de bureau, des ordinateurs portables ou des dispositifs de stockage amovibles.

La portée comprenait la période allant de juillet 2013 à décembre 2014, mais on insiste davantage sur les éléments plus récents.

La vérification excluait l'évaluation de la planification de la continuité des activités et les activités liées à la sécurité des TI relevant de Services partagés Canada.

Le travail de vérification sur le terrain s'est principalement déroulé à l'administration centrale, mais les régions ont pu y contribuer au moyen d'un questionnaire qui leur a été envoyé.

Forces observées

Les forces suivantes ont été cernées durant la vérification :

- Gouvernance - Des postes essentiels chargés de la sécurité des TI, soit l'ASM et le CST, ont clairement été assignés et un comité de sécurité ministérielle facilite les relations de travail.
- Sensibilisation - La sécurité des TI est intégrée au programme de sensibilisation à la sécurité.

Constatations

Chacun des critères de vérification a été évalué selon une combinaison de preuves recueillies au cours de l'examen de documentation, d'analyses, d'entrevues et de révisions des processus. Lorsqu'un écart important a été observé entre un critère de vérification et les pratiques courantes, le risque associé à cet écart a été évalué afin d'élaborer une conclusion et de formuler des recommandations en vue d'apporter des améliorations.

Des observations ont été notées dans les domaines suivants pendant la vérification :

- Sensibilisation à la sécurité des TI;
- Gestion des incidents liés à la sécurité des TI;
- Cadre stratégique;
- Gouvernance;
- Planification et gestion du risque;
- Conformité;
- Rapports internes;
- Accès aux applications et aux données.

Conclusion

La vérification a révélé que, bien que certains éléments que l'on pourrait espérer d'un programme de sécurité des TI sont en place, il est possible d'améliorer le cadre de gouvernance en ce qui concerne les exigences de la politique sur la sécurité des TI, la responsabilité relative à la sécurité des TI dans les régions, la gestion des risques et la planification proactive, ainsi que la vérification continue de la conformité aux exigences du gouvernement fédéral. Il est également possible d'améliorer certains contrôles de l'accès liés aux applications et aux données. Le travail de vérification a donné lieu à sept recommandations.

Énoncé de conformité

La vérification de la sécurité des technologies de l'information est conforme aux *Normes de vérification interne du gouvernement du Canada*, comme en témoignent les résultats du programme d'assurance et d'amélioration de la qualité.

Résumé des critères de vérification	
1.	Gouvernance relative à la sécurité des TI
1.1	Des politiques sur la sécurité des TI harmonisées avec le cadre stratégique du gouvernement en matière de sécurité des TI ont été élaborées et communiquées au sein du Ministère.
1.2	Des organismes ministériels de surveillance pour la gestion de la sécurité des TI ont été créés.
1.3	Un plan courant de la sécurité des TI existe et cadre avec les priorités pangouvernementales.
1.4	Un plan des ressources humaines pour le personnel de la sécurité des TI existe et cadre avec les priorités et les plans.
1.5	Une approche ministérielle de gestion des risques liés à la sécurité des TI a été mise en œuvre.
1.6	La production de rapports sur la conformité et le rendement associé à la sécurité des TI contribue à la prise de décision.
2.	Pratiques relatives à la sécurité des TI concernant les données ministérielles
2.1	Des contrôles sont en place pour restreindre l'accès aux applications et aux partages réseau.
2.2	Des contrôles sont en place pour restreindre l'accès aux comptes privilégiés.
2.3	Un nouveau programme de sensibilisation à la sécurité est en vigueur.
2.4	Il existe un processus pour gérer efficacement les incidents liés à la sécurité des TI qui comprend l'identification, la détection et les procédures en matière de réponse et récupération.