Relations Couronne-Autochtones et Affaires du Nord/Services aux Autochtones Canada

Rapport de vérification interne final

Vérification de la sécurité des TI

Rédigé par :

Direction générale des services de vérification et d’assurance

Mars 2018

TABLE DES MATIÈRES

Acronymes……ii
Contexte....1
Objectif de la vérification....2
Portée de la vérification....2
Observation positives....2
Constatations....3
Conclusion....3
Déclaration de conformité....3
Résumé des critères de vérification....3

Acronymes

AANC	Affaires autochtones et du Nord Canada
AC	Administration centrale
ASM	Agent de sécurité du Ministère
CST	Centre de la sécurité des télécommunications`
CT	Conseil du Trésor
DPI	Dirigeant principal de l'information
GC	Gouvernement du Canada
GRSTI	Gestion des risques pour la sécurité des technologies de l'information
GSTI	Norme opérationnelle de sécurité : gestion de la sécurité des technologies de l'information
SPC	Services partagés Canada
TI	Technologies de l'information
USB	Bus sériel universel

Contexte

La vérification de la sécurité des technologies de l'information (TI) était incluse dans le plan de vérification axé sur le risque de 2017-2018 à 2019-2020 d'AANC approuvé par la sous-ministre le 13 mars 2017. Elle avait été qualifiée de prioritaire au motif que la sécurité des TI est complexe et essentielle aux activités du Ministère, en plus d'être très délicate et d'avoir un potentiel de risque élevé. La sécurité des TI est responsable de protéger les renseignements personnels et de nature délicate. Quant aux systèmes des TI, ils font partie de l'infrastructure essentielle du Ministère.

La sécurité des TI est l'ensemble des mesures prises pour préserver la confidentialité, l'intégrité, la disponibilité, l'utilisation prévue et la valeur des renseignements conservés, traités ou transmis par voie électronique. Elle comprend également les mesures de sécurité qui s'appliquent aux biens utilisés pour recueillir, traiter, stocker ou détruire les renseignements électroniques. Les TI et leur sécurité sont un procédé continu, car les serveurs sont actifs 24 heures par jour, 365 jours par année. Il y a eu une augmentation constante de l'utilisation des ressources technologiques pour traiter, stocker et transmettre les renseignements afin d'appuyer la prestation continue des programmes. Le recours accru du Ministère aux TI souligne la nécessité de protéger les renseignements et d'avoir des contrôles et des pratiques solides en matière de sécurité des TI.

Récemment, il y a eu un nombre important et sans cesse croissant de cas d'atteintes à la sécurité des données signalés au Canada et qui touchent les Canadiens. Des cyberattaques touchant précisément le gouvernement du Canada (GC) ont notamment ciblé le Conseil national de recherches du Canada, le ministère des Finances, le ministère de la Défense nationale et le Secrétariat du Conseil du Trésor. En plus des cyberattaques, d'autres incidents importants sont survenus à maintes reprises en ce qui concerne la sécurité et la fonctionnalité des systèmes et des services des TI.

À l'heure actuelle, le GC normalise, consolide et restructure la manière dont il fonctionne à l'interne. Dans le cadre de la stratégie de modernisation des TI du GC[1], Services partagés Canada (SPC) a été créé en 2011 pour maintenir et améliorer la prestation du service des TI, réaliser des économies et mettre en œuvre des solutions modernes, fiables et sécuritaires dans l'ensemble du gouvernement. La gouvernance de la sécurité des TI s'est nécessairement complexifiée, car il s'agit désormais d'une responsabilité partagée entre SPC et les autres ministères. SPC est responsable du périmètre de défense d'AANC, de la gestion des réseaux, de la gestion du stockage et de l'optimisation des serveurs. AANC demeure responsable de la gestion et de la sécurité des ordinateurs de bureau, des applications de bases de données et de l'information.

En tant que ministère fédéral, AANC est régi par la *Politique sur la sécurité du gouvernement* (PSG) de 2012 du CT. Outre cette politique, le CT a émis en 2009 une *Directive sur la gestion de la sécurité ministérielle*, selon laquelle les ministères doivent avoir une politique de sécurité ministérielle. Examinant davantage les renseignements et la sécurité des TI, la *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (*GSTI) de 2004 du CT définit les exigences sécuritaires de base que les ministères fédéraux doivent respecter afin d'assurer la sécurité de l'information et des biens des TI placés sous leur contrôle. Par ailleurs, le Centre de la sécurité des télécommunications Canada (CSTC) a émis

[1] *Plan stratégique des technologies de l'information du Gouvernement du Canada*

en 2012 le *Conseil 33 en matière de sécurité des technologies de l'information* (ITSG-33) concernant la gestion des risques liés à la sécurité des TI. Il est important de noter que l'utilisation de la GSTI est éliminée progressivement tandis que celle de l'ITSG-33 devient plus largement appliquée.

Un programme de sécurité efficace combine des outils et des technologies avec la formation et la sensibilisation des utilisateurs pour protéger les renseignements et les systèmes, ainsi que la coordination par une variété d'intervenants. À AANC, les deux principaux responsables de la sécurité des TI, qui exercent des rôles essentiels, sont le dirigeant principal de l'information (DPI), en charge de la Direction générale de la gestion de l'information du Secteur du Dirigeant principal des finances, des résultats et de l'exécution, qui est responsable de la sécurité des TI et est appuyé par un coordonnateur de la sécurité des TI, selon la GSTI, et l'agent de sécurité du Ministère (ASM), dont la responsabilité incombe au directeur, Sécurité et aménagement des locaux, au sein de la Direction générale des services de ressources humaines et du milieu de travail.

La vérification a été complétée avant la dissolution d'AANC et la création de Relations Couronne-Autochtones et Affaires du Nord (RCAAN) et de Services aux Autochtones Canada (SAC). Les constatations et les recommandations de ce rapport s'appliquent aux deux Ministères.

Objectif de la vérification

L'objectif de la vérification était d'évaluer la conformité du Ministère aux composantes pertinentes de sécurité des TI de la Politique sur la sécurité du gouvernement du SCT et de la GSTI, ainsi que les cadres de contrôle pertinents en vigueur afin d'atténuer les risques en matière de sécurité des TI.

Portée de la vérification

La portée de la vérification incluait une évaluation de la pertinence et de l'efficacité des contrôles de gestion et des contrôles opérationnels et techniques en vigueur pour la sécurité des TI afin de protéger les renseignements et les biens ministériels des TI. La vérification comprenait la coordination et les communications entre Services partagés Canada (SPC) et AANC en ce qui concerne les processus de cyber sécurité, mais excluait un examen direct des activités de SPC puisque ce n'était pas une vérification conjointe avec SPC. Par conséquent, cette vérification fournit une assurance sur les activités de sécurité des TI d'AANC. Cependant, il est prévu qu'AANC travaillera conjointement avec SPC pour réaliser les recommandations incluses dans ce rapport.

L'équipe de vérification a réalisé des travaux sur le terrain à l'Administration centrale (AC) d'AANC et dans deux bureaux régionaux (Québec et Ontario); un autre bureau régional a été contacté par téléconférence (Colombie-Britannique). La vérification comprenait également l'essai des principales applications d'AANC.

Observation positives

Les points forts suivant ont été identifiés lors de la vérification:

- Les documents secrets sont gérés efficacement;

- Des outils sont en place pour empêcher les logiciels malveillants d'infecter les postes de travail et le Ministère a mis en place un filtrage des services de stockage dans le nuage pour empêcher le stockage non autorisé de documents dans le nuage; et
- AANC a officialisé les rôles d'agent de sécurité régional et de gestionnaire régional de l'information en matière de sécurité des TI.

Constatations

À partir des éléments probants recueillis au cours de l'examen de la documentation, de l'analyse et des entrevues, chacun des critères de vérification a été évalué et des conclusions en ont été tirées. Lorsqu'une différence importante était relevée entre le critère de vérification appliqué et la pratique observée, le risque résultant de cet écart était évalué; cette évaluation servait alors à tirer une conclusion et à formuler des recommandations pour des initiatives d'amélioration.

Des observations ont été notées dans les domaines suivants au cours de la vérification :

- gestion de la surveillance de la sécurité;
- gestion des renseignements de nature délicate;
- gestion des accès utilisateurs;
- développement et mise en œuvre d'applications de TI protégées;
- continuité des TI.

Conclusion

La vérification a permis de conclure que même s'il existe des contrôles de gestion clés liés à la sécurité des TI, des opportunités existent dans les domaines suivants : la gestion de la surveillance de la sécurité, la gestion des renseignements de nature délicate, la gestion des accès utilisateurs, le développement et la mise en œuvre d'applications de TI protégées et la continuité des TI. La vérification a donné lieu à cinq recommandations.

Déclaration de conformité

La vérification a été effectuée conformément aux *Normes internationales pour la pratique professionnelle de la vérification interne*, comme en font foi les résultats du programme d'assurance et d'amélioration de la qualité.

Résumé des critères de vérification

Afin de garantir le niveau d'assurance approprié pour répondre aux objectifs de la vérification, les critères de vérification ci-dessous ont été élaborés.

Critères de vérification	
1. Des contrôles de gestion efficaces de la sécurité des TI sont en place pour respecter les exigences stratégiques et atténuer les risques.	
1.1	Les rôles et les responsabilités associés à la sécurité des TI entre la DGGI, les régions et SPC sont clairement définis et communiqués.
1.2	Un plan de sécurité des TI a été déployé en conformité avec le plan des TI pour tenir compte des risques de sécurité des TI et des exigences de conformité (Les 10 mesures du CST, AMPS).
1.3	Le ministère s'assure que les processus appropriés sont en place pour respecter les instruments de politique sur la Sécurité des TI.
2. Des contrôles opérationnels et techniques de la sécurité des TI efficaces sont en place pour respecter les exigences stratégiques et atténuer les risques.	
2.1	Un processus efficace est en place pour déceler les incidents et rétablir les activités dans les meilleurs délais.
2.2	Les systèmes de TI et les sauvegardes permettent de gérer efficacement les renseignements classifiés.
2.3	Les activités des bureaux régionaux sont conformes aux exigences de l'AC.
2.4	Des sauvegardes efficaces sont en place pour protéger les renseignements électroniques de nature délicate d'AANC contre les cyberattaques.
2.5	Un processus efficace est en place pour rétablir les activités dans les meilleurs délais après des sinistres des TI.