Santé Canada et l'Agence de la santé publique du Canada
Health Canada and the Public Health Agency of Canada
Canada

Sommaire

Audit de la sécurité des technologies de l'information (TI) à l'Agence de santé publique du Canada et à Santé Canada

Mars 2017

Version traduite. En cas de divergence entre le présent texte et le texte anglais, la version anglaise a préséance.

1. Contexte

Les technologies de l'information (TI) sont un bien stratégique et un outil essentiel permettant au gouvernement du Canada de donner suite à son engagement consistant à fournir aux Canadiens des services intégrés et facilement accessibles tout en s'assurant que les opérations administratives internes sont gérées de façon efficace et efficiente. *La Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information* (GSTI) du Secrétariat du Conseil du Trésor (SCT) du Canada définit la sécurité des TI 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. Pour les besoins du présent audit, la « sécurité des TI » comprend tout ce qui porte sur la sécurité des renseignements électroniques, quelque que soit le support, y compris la cybersécurité.

Les services administratifs ministériels, qui comprennent les services des TI, relèvent de l'Entente-cadre de Partenariat de services partagés entre Santé Canada (SC) et l'Agence de la santé publique du Canada (ASPC). En vertu de cette entente, la Direction des services de gestion de l'information (DSGI) de la Direction générale des services de gestion (SC) est responsable de la mise en place et du maintien de l'infrastructure des TI pour utilisateurs finaux (p. ex. informatique de bureau). La DSGI est également responsable du développement et du maintien des applications logicielles à l'appui des programmes et des services. Actuellement, la fonction ministérielle de sécurité des TI relève du directeur exécutif de la Prestation des services des TI. La responsabilité de tous les aspects de la sécurité, notamment de la sécurité des TI, incombe à l'agent de sécurité du Ministère (ASM). Le coordonnateur de la sécurité des TI (CSTI) est responsable de la gestion du programme de sécurité des TI.

Les services administratifs ministériels, qui comprennent les services des TI, relèvent de l'Entente-cadre de Partenariat de services partagés entre Santé Canada (SC) et l'Agence de la santé publique du Canada (ASPC). En vertu de cette entente, la Direction générale des services de gestion (SC) assure les services de sécurité. La responsabilité de tous les aspects de la sécurité, notamment de la sécurité des TI, incombe à l'agent de sécurité du Ministère (ASM). Le coordonnateur de la sécurité des TI (CSTI) est responsable de la gestion du programme de sécurité des TI.

On compte également des systèmes de TI à SC et à l'ASPC qui ne relèvent pas de la DSGI ou de SPC. Ce sont des systèmes qui ont été déployés et sont exploités au sein des deux organismes qui ne sont pas gérés par la DSGI. Le Réseau de la science du Bureau de la radioprotection, sous l'égide de la Direction générale de la santé environnementale et de la sécurité des consommateurs à SC et le Réseau de la bioinformatique au Laboratoire national de microbiologie (LNM) à Winnipeg, sous l'égide de la Direction générale de la

prévention et du contrôle des maladies infectieuses à l'ASPC sont des exemples de réseaux de TI qui sont distincts du réseau ministériel de SC et de l'ASPC et ne communiquent pas avec ces derniers.

2. Objectif de l'audit

L'audit avait pour objet d'évaluer l'efficacité du cadre de contrôle de gestion pour ce qui est de la gestion de la sécurité des TI au sein de SC et de l'ASPC et du respect des politiques, directives et normes du SCT et du Ministère.

3. Portée de l'audit

La portée de l'audit comprenait un examen des principaux processus et pratiques en place pour gérer la sécurité des TI et le niveau des mesures de protection techniques et opérationnelles existant à SC et à l'ASPC. L'audit comprenait un examen de l'infrastructure des TI, des services des TI, des applications et systèmes du Ministère et de la gestion de l'information électronique relevant de SC et de l'ASPC.

L'infrastructure et les services des TI fournis par Services partagés Canada (SPC) et d'autres fournisseurs de services tiers ont été exclus de l'audit puisqu'ils ne relèvent pas de SC et de l'ASPC. La portée de l'audit excluait aussi la continuité des TI pour les applications et systèmes essentiels à la mission, la sécurité du personnel et matérielle, ainsi que les mesures de protection concernant les dossiers papier, puisque ces sujets ont récemment été abordés dans d'autres audits.

L'audit portait du 1er avril 2015 au 30 septembre 2016.

4. Méthode de l'audit

L'audit a permis d'examiner les pratiques de gouvernance, de gestion des risques et de contrôle dans le cadre de la gestion de la sécurité des TI au sein de SC et de l'ASPC et de comparer ces pratiques à des critères d'évaluation prédéfinis. L'approche d'audit comprenait un examen de la documentation, des politiques, des normes, des lignes directrices, des cadres et des processus opérationnels. Des entrevues ont été menées auprès de responsables clés de la DGSG et du LNM. Des entrevues ont également été menées auprès de l'agent de sécurité du Ministère (ASM) et d'autres représentants ministériels de secteurs de programme. L'audit a permis d'examiner les rôles, les responsabilités et la responsabilisation dans le cadre de la gestion de la sécurité des TI au sein de SC et de l'ASPC. Enfin, l'audit a permis de mettre à l'essai, d'analyser et d'examiner les contrôles internes de la GI-TI en vue de s'assurer que les contrôles clés en matière de sécurité des TI étaient présents dans le cadre de la gestion des biens ministériels de la GI-TI. L'audit a été mené dans la région de la capitale nationale et à Winnipeg.

5. Constatations

Des recommandations ont été formulées dans les domaines de la gouvernance, de la gestion du risque et du contrôle. La gestion a rédigé la réponse de la direction et le plan d'action en vue de donner suite aux recommandations.

6. Énoncé de conformité

Selon le jugement professionnel du dirigeant principal de l'audit, les procédures ont été effectuées et des preuves ont été recueillies de façon suffisante et appropriée afin d'assurer l'exactitude de la conclusion de l'audit. Les résultats et la conclusion de l'audit sont fondés sur une comparaison des conditions qui existaient au moment de l'audit avec les critères de vérification convenus avec la direction. De plus, les renseignements probants ont été réunis conformément aux *Normes relatives à la vérification interne au sein du gouvernement du Canada* et aux *Normes internationales pour la pratique professionnelle de la vérification interne*. L'audit respecte les *Normes relatives à l'audit interne au sein du gouvernement du Canada*, comme viennent l'appuyer les résultats du programme d'amélioration et d'assurance de la qualité.