Santé Canada Health Canada

Rapport de vérification définitif

Vérification de la Sécurité des technologies de l'information (TI)

Mars 2011

Table des matières

Sommaire

Selon la *Politique sur la sécurité du gouvernement,* la sécurité de la technologie de l'information (TI) renferme des «mesures de protection» de la confidentialité, de l'intégrité, la disponibilité, l'utilisation recherchée et la valeur de l'information entreposée, traitée ou transmise électroniquement. En 2005, le Secrétariat du Conseil du Trésor du Canada avait exigé de tous les ministères qu'ils appliquent la Norme de gestion de la sécurité des technologies de l'information (GSTI) d'ici décembre 2006. Cette norme de sécurité opérationnelle est le fondement de toutes les normes de sécurité des TI que tous les ministères fédéraux doivent respecter.

Cette vérification avait pour but d'évaluer les contrôles internes mis en place à l'appui de la sécurité des TI stipulés dans la Norme de gestion de la sécurité des technologies de l'information (GSTI). La vérification a évalué en particulier : l'Organisation de la sécurité des TI, la politique et le Programme de sécurité des TI du Ministère, les Contrôles de la sécurité des TI et les mesures de protection opérationnelles et techniques.

Selon le jugement professionnel du dirigeant principal de la vérification, des procédures suffisantes et convenables ont été suivies et la preuve a été réunie pour appuyer l'exactitude des conclusions de la vérification. Les constatations et la conclusion de la vérification sont basées sur une comparaison des conditions qui existaient à la date de la vérification aux critères établis en accord avec la direction. De plus, la preuve a été réunie conformément aux *Normes de vérification interne pour le gouvernement du Canada* et aux *Normes internationales pour les méthodes professionnelles de vérification interne.*

En ce moment, Santé Canada ne s'est pas encore tout à fait conformé à la norme de sécurité opérationnelle même si le Ministère a consacré d'importantes ressources pour atteindre la norme prescrite par la GSTI. Atteindre cette norme fondamentale a présenté un grand défi pour le gouvernement et quelques ministères y ont réussi. Malgré cette difficulté à surmonter, Santé Canada a reçu une note *acceptable* lors de l'évaluation de son cadre de responsabilisation de gestion en 2009-2010. Historiquement, la Direction des services de gestion de l'information a réalisé des progrès dans l'identification des lacunes des TI et des contrôles de l'information et elle a déterminé les endroits où ces contrôles devaient être renforcés et plus efficaces. Même si des « lacunes » concernant les Contrôles de la sécurité des TI ont été décelées, il est davantage nécessaire de les corriger. Il existe donc certaines zones vulnérables sur lesquelles il faut se pencher afin de renforcer encore plus la posture de sécurité des TI du Ministère. (Voir l'Annexe B – Feuille de pointage)

Le rapport comprend sept (7) recommandations visant à renforcer la sécurité des TI à Santé Canada. La direction souscrit à chacune des recommandations et a préparé un plan d'action pour chacune.

1. Introduction

1.1 Contexte

Selon la *Politique de sécurité du gouvernement*, la sécurité de la technologie de l'information (TI) renferme des «mesures de protection» de la confidentialité, de l'intégrité, l'admissibilité, l'utilisation recherchée et la valeur de l'information entreposée, traitée ou transmise électroniquement. Depuis 2002, le Secrétariat du Conseil du Trésor du Canada a collaboré avec les principales agences de sécurité et avec certains ministères pour rédiger plusieurs normes de sécurité opérationnelles et techniques que ces derniers devront respecter pour assurer la sécurité de l'information et des biens liés à la technologie de l'information sous son contrôle. En 2005, le Secrétariat du Conseil du Trésor du Canada avait exigé de tous les ministères qu'ils appliquent les normes opérationnelles de *Gestion de la sécurité des technologies de l'information* (GSTI), d'ici 2006, comme exigence fondamentale à leur programme de sécurité des TI. Satisfaire à cette exigence fondamentale s'est révélé un défit pour le gouvernement et la plupart des ministères ont reçu la note « *acceptable* » de l'évaluation de responsabilisation de gestion du Secrétariat du Conseil du Trésor du Canada pour l'exercice 2009-2010 en signalant que le Ministère avait atteint les trois (3) objectifs prioritaires du fondement de la Gestion de la sécurité des technologies de l'information (GSTI) et qu'il s'était conformé à la plupart de ses exigences.

Le degré de protection que Santé Canada peut assurer à son propre programme de sécurité des TI influence directement sa capacité à fournir une prestation continue de services qui contribuent à la santé, à la sécurité et au bien-être économique des Canadiens contre un environnement de menace en constante évolution. La sécurité du réseau implique toutes les activités que Santé Canada entreprend pour protéger la valeur et l'utilisation continue des biens ainsi que de l'intégrité et la continuité des opérations. Une stratégie efficace de sécurité des TI exige de déceler les menaces et de choisir l'ensemble d'outils le plus efficace pour les écarter. Il est nécessaire de veiller à ce que les personnes ayant accès à l'information, aux biens et aux services gouvernementaux y aient le droit. Santé Canada doit donc gérer de façon proactive les menaces, les risques et les incidents liés à la sécurité afin de protéger les biens, l'information et les services essentiels pour atteindre ses objectifs stratégiques.

1.2 Objectif de la vérification

L'objectif de cette vérification visait à évaluer les contrôles internes existants de la sécurité des TI à Santé Canada stipulés dans la Norme de gestion de la sécurité des technologies de l'information (GSTI). La vérification a insisté en particulier sur la sécurité des TI liée :

- à l'organisation de la sécurité des TI;
- à la politique ministérielle en matière de sécurité des TI;
- aux contrôles de la sécurité des TI;
- aux mesures de protection opérationnelles et techniques.

1.3 Portée et méthode

La norme 12.11.2 de la *Gestion de la sécurité des technologies de l'information* (GSTI) précise que la planification de la sécurité des technologies de l'information (TI) est nécessaire. Comme la sécurité des TI appartient au monde de la vérification, elle a donc été intégrée au processus de planification de vérification interne du Ministère. La vérification de la sécurité des TI a été entreprise par le Bureau de la vérification et de la responsabilisation, conformément au Plan de vérification axé sur le risque pour les exercices de 2009-2010 à 2011-2012 du Ministère qui a reçu l'appui du Comité ministériel de vérification le 22 mai 2009 pour être par ensuite approuvé par le sous-ministre.

En janvier 2007, le Conseil du Trésor a changé le format du rapport de situation de la GSTI, réduisant à environ 50 les 144 éléments qu'il comprenait. Même si la vérification a, en grande partie, respecté cette nouvelle exigence, les 50 éléments n'ont pas tous été examinés. Une évaluation du risque pour examiner les principales sections de la norme a été réalisée. Les résultats obtenus ont été utilisés pour concentrer la vérification sur des sections du Ministère où les risques étaient les plus élevés. Les critères d'évaluation provenaient de la norme de GSTI et du *Control Objectives for Information and Related Technology* (COBIT).

La vérification a été réalisée dans la région de la capitale nationale. La phase de l'enquête comprenait des entrevues avec des représentants de la Direction générale des services de gestion et de la Direction générale des régions et des programmes. Cette phase comprenait également une révision des dossiers et un examen de documents choisis, notamment ceux portant sur des évaluations de menaces, de risques et de vulnérabilités, des énoncés de sensibilité, des évaluations des répercussions sur la vie privée, des politiques, des normes, des lignes directrices, des accords de niveau de services, des cadres de travail et des plans.

La vérification n'a pas touché aux sections de normes de sécurité opérationnelles liées à la santé et à la sécurité professionnelles, à la sécurité physique, au sans fil ni à la planification de la continuité des activités. La planification de la continuité des activités a fait l'objet d'une vérification interne à Santé Canada et a été déposée en décembre 2010, et le sans-fil a été vérifié à l'externe récemment par le Commissaire à la protection de la vie privée.

1.4 Énoncé d'assurance

Selon le jugement professionnel du dirigeant principal de la vérification, des procédures suffisantes et convenables ont été suivies et la preuve a été réunie pour appuyer l'exactitude des conclusions de la vérification. Les constatations et la conclusion de la vérification sont basées sur une comparaison des conditions qui existaient à la date de la vérification aux critères établis en accord avec la direction. De plus, la preuve a été réunie conformément aux *Normes de vérification interne pour le gouvernement du Canada* et aux *Normes internationales pour les méthodes professionnelles de vérification interne.*

2. Constatations, recommandations et réponses de la direction

2.1 Organisation de la sécurité des TI

2.1.1 Structure de gouvernance

Critère de vérification : *Il devrait exister un cadre de gouvernance pour la sécurité des TI.*

La structure de gouvernance de la GI/TI de Santé Canada comprend quatre (4) organismes de surveillance : le Comité exécutif de gestion, son sous-comité des opérations et la Direction des services de gestion de l'information - Comité exécutif. Le comité au niveau de la Direction est appuyé par deux groupes de travail : le Comité de gestion des opérations et le Comité de supervision des opérations. Au moment de la vérification, le quatrième organisme de surveillance était le Comité de responsabilisation pour la gestion de l'information (CRGI) qui était formé en tant que conseil pseudo consultatif composé de clients de la Direction des services de gestion de l'information (DSGI) au niveau exécutif.

La sécurité des TI reçoit également une aide supplémentaire de la part d'un organisme consultatif externe. Le Centre canadien de réponse aux incidents cybernétiques (CCRIC), qui est régi par Santé publique et protection civile Canada, aide tous les ministères et organismes fédéraux. Le Centre canadien de réponse aux incidents cybernétiques est chargé de surveiller de façon ininterrompue les cybermenaces et de coordonner la réponse nationale à tout incident de sécurité cybernétique. Il donne la priorité à la protection des infrastructures nationales essentielles contre les incidents cybernétiques. Tous les résultats intéressant Santé Canada sont communiqués à l'agent de sécurité ministériel afin qu'il prenne les mesures nécessaires. Santé Canada s'appuie aussi sur le Centre de la sécurité des télécommunications Canada (CSTS), sur le Service canadien du renseignement de sécurité (SCRS) et sur la Gendarmerie royale du Canada (GRC) pour les compétences et les renseignements en matière de sécurité des TI.

2.1.2 Principaux rôles et principales responsabilités

Critère de vérification : *Les postes de la haute direction définis dans la norme opérationnelle sur la sécurité devraient être créés au Ministère.*

La Direction des services de gestion de l'information de la Direction générale des services de gestion offre des services de TI à la grandeur du Ministère et assume la responsabilité des principaux éléments de l'infrastructure des TI de Santé Canada. Celui-ci possède un coordonnateur de la sécurité des TI (CSTI) qui relève directement du dirigeant principal de l'information et (fonctionnellement) à l'agent de sécurité ministériel qui, tous les deux, travaillent vers l'assurance d'un leadership pour la posture de la sécurité des TI du Ministère. Chacun de ces postes relève directement du sous-ministre adjoint de la Direction générale des services de gestion. De plus, Santé Canada dispose de six bureaux régionaux et chacun d'eux possède son groupe de sécurité des TI. Toutes ces personnes relèvent du sous-ministre adjoint de la Direction générale des régions et des programmes. Les rôles et les responsabilités sont décrits dans la Directive de sécurité des TI et leur dernière mise à jour remonte à décembre 2006.

Le dirigeant principal de l'information (DPI) est responsable des travaux de la Direction des services de gestion de l'information. Tel que la norme de sécurité des TI le prévoit, le DPI travaille en étroite collaboration avec le coordonnateur de la sécurité de TI afin d'assurer une gestion efficiente et efficace de la sécurité des TI du Ministère et que des mesures de sécurité pertinentes sont appliquées à toutes les activités, à tous les processus et à tous les biens des TI.

Le sous-ministre a délégué le directeur de la sécurité des TI d'agir en tant que le coordonnateur de la sécurité ministériel des TI. Il incombe à ce dernier de collaborer avec l'agent de sécurité ministériel touchant la sécurité des TI. Le coordonnateur de la sécurité ministériel des TI fournit en premier lieu une orientation globale aux programmes de sécurité technique et agit à titre de point de contact ministériel des principaux organismes du gouvernement du Canada concernant la sécurité des technologies de l'information. Ces responsabilités sont comparables à celles décrites dans la norme de sécurité. Un personnel de 21 employés soutient en ce moment le coordonnateur de la sécurité des TI.

Le sous-ministre a délégué le directeur exécutif de la Division de la gestion de la sécurité et des mesures d'urgence comme agent de sécurité ministériel. Il est responsable de la direction générale des programmes concernant la sécurité à l'intérieur de Santé Canada. La conformité à ces dispositions est obligatoire telle que le stipule, la *Politique de sécurité du gouvernement* et ses documents à l'appui annexes décrits dans les *Normes de sécurité opérationnelles* du Conseil du Trésor.

Comme il a été écrit précédemment, Santé Canada compte six bureaux régionaux possédant leur propre groupe de sécurité des TI. Ces employés relèvent du sous-ministre adjoint de la Direction générale des régions et des programmes. Un examen régional de la sécurité des TI a été réalisé en révisant des documents régionaux et en menant des entrevues avec le personnel de la sécurité de l'information des régions. [redacted].

Recommandation 1

Il est recommandé au sous-ministre adjoint de la Direction générale des services de gestion, autorité fonctionnelle de la sécurité des TI, de collaborer avec les directions générales [redacted] *réponde aux exigences de Santé Canada en matière de sécurité.*

Réponse de la direction

La direction souscrit à la recommandation.

[redacted]

[redacted]

2.2 Politique et programme de sécurité des TI

2.2.1 Politique de sécurité des TI

Critère de vérification : *Santé Canada devrait avoir une politique de sécurité des TI appuyée par un programme de sécurité des TI.*

Un programme de sécurité des TI efficace comporte trois volets interdépendants – une politique de sécurité des TI (contenant des déclarations claires qui appuient les objectifs opérationnels et de sécurité du Ministère), des praticiens de la sécurité des TI qualifiés et compétents (qui assurent l'orientation, l'interprétation et l'application de ces objectifs de la politique) et une intégration fonctionnelle dans les services de TI du Ministère. Même si Santé Canada a élaboré ces trois entités à divers degrés de maturité, elles ne sont pas effectivement synchronisées comme un programme de sécurité des TI devrait l'être afin de protéger l'information et les biens de l'information. Le Ministère a élaboré et documenté des politiques et des procédures ministérielles qui fourniraient un cadre de travail à la mise en œuvre d'un tel programme. Ce programme pourrait tenir compte des évaluations des risques, de la planification de la sécurité des systèmes d'information (notamment les exigences actuelles et prévues en matière de sécurité des TI), des stratégies d'essai courantes pour évaluer les contrôles de sécurité et déterminer l'efficacité des politiques et des procédures de sécurité des TI, des plans d'action correctifs qui détermineraient les ressources nécessaires pour rectifier ou atténuer les faiblesses connues de la sécurité accompagnés d'un inventaire complet et précis des systèmes.

Le projet de conformité à la GSTI 2006-2007 de Santé Canada a été utilisé pour élaborer les exigences de la politique de sécurité des TI. Il existe plusieurs directives et outils touchant la sécurité des TI à l'appui de cette politique. Cependant, certaines de ces directives qui apparaissent sur le site Intranet de Santé Canada ne contiennent que des titres sans textes explicatifs auxquels est affichée l'épithète « préliminaire » ou en « voie de réalisation ».

Récemment, le programme de sécurité des TI s'est uni sous une unité unique de gestion avec un mandat pour mieux intégrer la sécurité au sein des fonctions de la TI de la DSGI. Administrer

les activités ci-dessus vers la création d'un programme intégré de sécurité des TI sous un unique gestionnaire est l'endroit logique pour compléter ce processus.

Recommandation 2

Il est recommandé au sous-ministre adjoint de la Direction générale des services de gestion, d'élaborer et de documenter un programme de sécurité des TI conformément à la Politique sur la sécurité des TI de Santé Canada.

Réponse de la direction

La direction souscrit à la recommandation.

[redacted]

2.3 Contrôles de la sécurité des TI

2.3.1 Gestion du cycle de vie des applications

Critère de vérification : *L'architecture des contrôles de la gestion de la sécurité des TI devrait inclure tous les aspects du cycle de vie du développement d'un système comme une responsabilité partagée entre la sécurité des TI et les propriétaires d'entreprises.*

Les propriétaires d'entreprises doivent tenir compte des questions de sécurité liées à une nouvelle application dès le début du cycle de vie du projet et travailler en étroite collaboration

avec la sécurité des TI afin de miser sur les concepts d'une « solide approche du cycle de vie du développement d'un logiciel ». Essayer de mettre en œuvre des contrôles de sécurité à la fin d'un cycle de vie mène à des pertes de temps et d'argent. En utilisant le *Registre des logiciels d'application*, l'équipe de la sécurité des TI peut gérer les exigences en matière de sécurité tout au long des étapes du cycle de vie des applications.

Le *Registre des logiciels d'application* est une application Web qui facilite la collecte d'information de tous les systèmes et de toutes les applications à Santé Canada et qui appuie également la capacité du Ministère à gérer l'information sur ses applications tout au long du cycle de vie du développement d'un système. La Division du développement des applications et de l'Internet (DDAI), les Services de sécurité des TI et le Projet de GSTI se sont réunis pour développer une nouvelle approche afin d'obtenir de meilleurs taux de respect de la sécurité des applications ajoutées au réseau de Santé Canada. Grâce à une inscription simplifiée des applications et à un énoncé des processus de sensibilité, les propriétaires d'entreprises pourront se conformer rapidement et simplement aux exigences de la *Norme de la Gestion de la sécurité des technologies de l'information* (GSTI) du Secrétariat du Conseil du Trésor. L'orientation des propriétaires fonctionnels est donnée dans la *Stratégie des TI – Orientation pour les propriétaires d'entreprises d'applications*.

Cependant, le nombre d'applications qui satisfait à un examen complet de sécurité demeure relativement faible (voir le tableau ci-dessous). Un problème récurrent provient du fait que les propriétaires d'entreprises de biens essentiels n'acceptent pas encore toutes les recommandations relatives à la sécurité ou n'ont pas encore approuvé les évaluations des menaces et des risques. La sécurité des TI n'a pas de mandat clair ni l'autorité pour exiger la conformité de la part des propriétaires fonctionnels. Il s'ensuit que les processus et les contrôles de sécurité des TI ne sont pas encore appliqués comme prévu. Le tableau suivant donne les résultats de l'essai de vérification durant la période d'examen :

Résultats de l'essai de vérification

Nombre d'applications enregistrées	Énoncés de sensibilité terminés	Évaluations des menaces et des risques terminées	Certifications terminées	Accréditations terminées
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

L'équipe de vérification a évalué [redacted] nouvelles applications en production depuis avril 2009 [redacted].

2.3.2 Gestion des risques à la sécurité

Critère de vérification : *Les ministères doivent gérer en permanence les risques à la sécurité de l'information et les biens de TI tout au long du cycle de vie des programmes et des services.*

La sécurité des TI utilise aussi le *Registre des logiciels d'applications* pour gérer les risques à la sécurité. Ces activités comprennent la spécification de la sensibilité de l'information et les biens

de TI, la réalisation d'évaluations des menaces et des risques et de certifications et d'accréditations de sécurité de tous les biens des TI. Ces contrôles sont nécessaires pour veiller à ce que le développement de nouvelles applications et les modifications apportées aux applications existantes n'entraînent pas de risques à la sécurité de l'environnement du réseau.

- Les **énoncés de sensibilité (ÉS)** constituent une première étape importante du processus d'évaluation des risques. Ces énoncés déterminent et classent par catégorie l'information et les biens connexes selon leur sensibilité (publique, protégée, secrète, etc.).
- Les **évaluations des menaces et des risques (ÉMR)** répondent à certaines questions, par exemple : Que faut-il protéger? Qui ou qu'est-ce qui peut constituer une menace ou une vulnérabilité? Quelles sont les implications lors de dommages ou de pertes et qu'elle en est la valeur pour le Ministère? Elles comprennent également des recommandations pour atténuer les risques à la confidentialité, à l'intégrité et à la disponibilité.
- La **certification de sécurité (CS)** est accordée après une évaluation complète pour déterminer si des caractéristiques techniques et non techniques de sécurité dans un système ou une application satisfont un ensemble particulier d'exigences en matière de sécurité. Le processus comprend aussi la détermination et l'acceptation des risques résiduels du propriétaire d'entreprise. L'accréditation de sécurité est l'autorisation officielle de gérer une activité du système des TI et l'acceptation du risque résiduel connexe.

Comme il a été signalé précédemment, l'inscription déclenche automatiquement une demande de la Section de la sécurité des TI d'une validation de l'énoncé de sensibilité et l'évaluation des menaces et risques. Lorsqu'il est justifié, un rapport de certification et d'accréditation sera préparé pour une application. Ceci est actuellement le processus et la DSGI continue de l'améliorer.

En raison du très grand nombre d'applications inscrites, la sécurité des TI applique un processus « rapide » pour obtenir des applications [redacted] à la suite d'un examen minimal. Malgré cette mesure et comme il a été signalé précédemment, le taux de respect est encore faible et certains logiciels demeurent sur le réseau après la date d'expiration déterminée par « l'autorité temporaire responsable de son fonctionnement ».

Recommandation 3

Il est recommandé au sous-ministre adjoint de la Direction générale des services de gestion, de collaborer avec tous les autres sous-ministres adjoints afin de se conformer aux contrôles du cycle de vie de développement d'un système afin de supprimer ou d'atténuer, ou les deux à la fois, une exposition de la sécurité des TI aux risques.

Réponse de la direction

La direction souscrit à la recommandation.

[redacted]

[redacted]

Recommandation 4

Il est recommandé au sous-ministre adjoint de la Direction générale des services de gestion, de collaborer avec les autres sous-ministres adjoints à l'élaboration de contrôles compensatoires visant à renforcer la nature conditionnelle et l'acceptation des recommandations relatives à la sécurité des TI admises par une autorité intérimaire pour utiliser le développement nouveau ou amélioré.

Réponse de la direction

La direction souscrit à la recommandation.

[redacted]

2.3.3 Gestion de l'inventaire

Critère de vérification : *La gestion de l'inventaire de l'information et des biens de TI devrait être identifié et classé par catégorie en utilisant les caractéristiques qui mettent en évidence la sensibilité, la criticité et toutes autres qualités qui reflètent la valeur pour l'organisation.*

Le Ministère utilise également le *Registre des logiciels d'application* pour gérer les applications qu'il accueille à son réseau et pour déterminer le mandat des applications ministérielles essentielles. La sécurité des TI utilise un processus ascendant pour déceler les biens essentiels dans le but de concevoir une méthodologie unique qui pourrait être reproductible et identifiable, basée sur le risque et qui pourrait surmonter les défis d'une vérification.

Le document *« Aperçu des biens de TI essentiels »* décrit le processus utilisé pour déterminer, traiter, classer et approuver les biens de TI essentiels. Le processus utilise les caractéristiques pour souligner la sensibilité, la criticité, la priorité et le sérieux des applications. En 2008, le processus a identifié les 54 principales applications essentielles d'un inventaire contenant plus de 2000 applications. De cette liste, une liste de 12 applications essentielles de niveau 1. Celles exigeant une disponibilité continue ou de 24 heures ou moins, ont été soumises au Comité de responsabilisation pour la gestion de l'information aux fins d'approbation en tant que la liste officielle du Ministère.

Actuellement, lorsque des programmes entrent des applications dans le *Registre des logiciels d'application*, ils ont déterminé si l'application était essentielle en ne vérifiant qu'une boîte à l'écran. Cette vérification constitue maintenant l'identificateur définitif d'un bien essentiel du Ministère même s'il n'existe aucune assurance que cette vérification soit basée sur les caractéristiques définies dans le document « *Aperçu des biens de TI essentiels* ».

La sécurité des TI reconnaît l'existence d'un défi et il est en voie de clarifier un processus pour déterminer celui qui doit prendre la décision finale concernant la criticité.

Recommandation 5

> *Il est recommandé au sous-ministre adjoint de la Direction générale des services de gestion, d'examiner et de réviser l'identification et la catégorisation des biens des TI essentiels afin de respecter les normes de sécurité.*

Réponse de la direction

La direction souscrit à la recommandation.

Santé Canada a déployé des efforts remarquables pour déterminer les 12 biens des TI essentiels prioritaires en se fondant sur les critères du Conseil du Trésor et de la Sécurité du publique afin de se conformer aux exigences de GSTI en 2008. À la suite de nouveaux mandats, (la grippe A H1N1) par exemple, des changements aux applications et aux technologies actuelles et à l'infrastructure ministérielle en évolution des TI, il a été nécessaire d'examiner les biens existants et éventuellement émergents des TI essentiels, de déterminer les composantes communes et de veiller à ce que ces biens puissent satisfaire aux exigences en matière de

confidentialité, d'intégrité et de disponibilité. Afin de mieux assurer la cohérence et l'inclusion du Ministère, la création de cette liste exigera la participation de tous. La nouvelle liste, actuellement sous forme d'ébauche, exigera aussi l'approbation des tous les SMA de Santé Canada afin de vérifier la participation.

2.3.4 Gestion de la vulnérabilité

Critère de vérification : *Les vulnérabilités touchant l'infrastructure des TI de Santé Canada qui influencent les programmes, les systèmes et la prestation des services par le Ministère doivent faire l'objet d'une évaluation permanente.*

Selon la norme de sécurité, les ministères géreront, sans interruption, les vulnérabilités de ses programmes, de ses systèmes et de ses services. De plus, l'évaluation interne du réseau devrait prévoir un examen de la configuration du serveur, des politiques de sécurité et de l'utilisation d'un terminal pour déterminer régulièrement les vulnérabilités du réseau.

Le Ministère dispose d'un outil d'évaluation des vulnérabilités capable de mener des évaluations régulières des vulnérabilités sur les serveurs de réseau. [redacted].

[redacted].

[redacted].

2.3.5 Ségrégation du réseau

Critère de vérification : *Le programme de sécurité des TI doit tenir compte de la ségrégation de l'architecture et de la stratégie de ses contrôles.*

Une stratégie de ségrégation pour la stratégie des TI comprend des objets tels que des rôles, des systèmes, des processus et une architecture de réseau. La sécurité du périmètre du Ministère est un effort réuni de gestion de la Section de la connectivité et des télécommunications de la Division des services du centre des données et de la Division des services de bureautique.

La stratégie et les politiques de la sécurité du périmètre doivent offrir une séparation des responsabilités alors que dans un même temps, la capacité d'une personne l'empêche de contrôler les principaux systèmes du réseau du Ministère, créant ainsi un point unique de défaillance. Malgré l'absence de lignes directrices et de rôles et de responsabilités officiels, le personnel de la sécurité du périmètre utilise les privilèges « basés sur les rôles » qui accordent l'accès nécessaire pour remplir ses tâches. De plus, les pare-feux du réseau procurent des mesures sans défaillance de redondance qui atténuent les risques. [redacted].

L'une des composantes architecturales d'une stratégie de ségrégation du réseau est sa segmentation. L'architecture du réseau de Santé Canada a été conçue de façon à écarter le réseau interne du Ministère des services accessibles de l'extérieur. La ségrégation des rôles et des responsabilités pour tous les postes responsables de la gestion opérationnelle de la sécurité du réseau est pertinente et comprend des ressources de soutien nécessaires pour prévenir un point unique de défaillance.

[redacted].

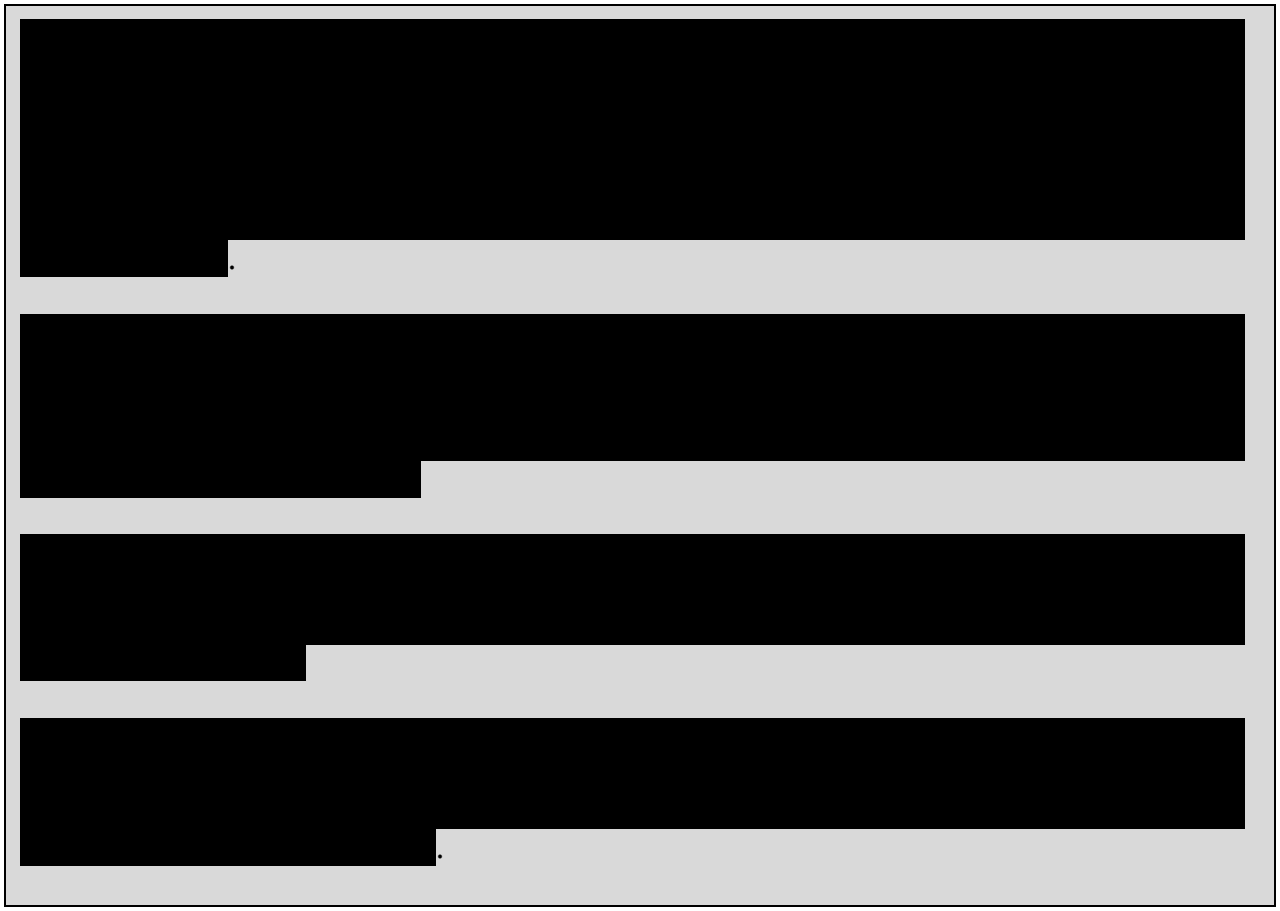
Recommandation 6

Il est recommandé au sous-ministre adjoint de la Direction générale des services de gestion, de terminer les évaluations des risques [redacted].

Réponse de la direction

La direction souscrit à la recommandation.

[redacted]



2.4 Mesures de protection opérationnelles et techniques

2.4.1 Stratégie de défense active

Critère de vérification : *Santé Canada devrait adopter une stratégie de défense active incluant la prévention, la détection, l'intervention et la récupération.*

Une stratégie de défense active implique plusieurs fonctions opérationnelles interdépendantes et des activités intégrées visant à procurer une sécurité de périmètre externe ainsi que des mesures de protection interne. La stratégie de défense active de Santé Canada comprend un programme de gestion des pare-feux, un programme de détection d'intrusion et de prévention, la gestion des retouches, l'authentification de l'utilisateur et les capacités d'accès à distance pour protéger le périmètre du réseau de Santé Canada.

La **gestion des pare-feux** exige la configuration, la coordination et la gestion des changements au terminal (serveurs et routeurs) dont le but est d'autoriser un trafic sur le réseau et de bloquer celui qui ne l'est pas. Les pare-feux doivent être configurés afin d'offrir la plus grande sécurité aux données sensibles, et les règles explicites des pare-feux devraient être mises en place pour permettre au trafic approprié de les traverser. Au cours des cinq dernières années environ, le Ministère a conclu un marché avec Travaux publics et Services gouvernementaux Canada (TPSGC) de services de pare-feux gérés et de filtrage des polluriels. Cependant,

[redacted] La DSGI signale que ceci était le résultat de processus et de protocoles de communication faibles entre Santé Canada et TPSGC. Il a donc fallu que le Ministère applique des mesures de protection supplémentaires pour réduire la probabilité que ces risques se reproduisent.

Les **services de détection d'intrusion et de prévention** font partie de la stratégie de défense active. Les principales responsabilités de la Section des technologies de la sécurité de la Division des services de bureautique consistent à mener des enquêtes légistes, à fournir une protection antivirus, à réaliser des évaluations des vulnérabilités complètes et à assurer des services de détection d'intrusion et de prévention. Cette équipe utilise un logiciel commercial standard et un terminal afin de procurer un niveau supérieur de protection contre des attaques sournoises qu'un pare-feu ne peut détecter.

La responsabilité de la détection d'intrusion et de prévention du réseau a été récemment transférée à la Section des communications et de l'interconnectivité. Un examen des journaux des préventions d'intrusion au niveau du réseau (serveurs) a démontré que ces contrôles préventifs [redacted]. Cependant, le niveau de complexité et de sophistication des agents adverses continue d'augmenter.

[redacted].

Gestion des retouches : La Section des technologies de la sécurité utilise, de façon régulière, le même produit logiciel pour supprimer les vulnérabilités des serveurs du réseau. Parmi les exemples de vulnérabilités atténuées qui utilisent la gestion des retouches, signalons l'intervention pour repousser des attaques de services lorsqu'un agresseur surcharge le système au moyen du trafic réseau dans une tentative pour réduire le système ou accroître le privilège d'attaquer lorsque l'agresseur trompe le système pour obtenir des privilèges supérieurs à ceux autorisés. Lors de la phase d'enquête de la vérification, [redacted], à mesure que le projet se déplace vers l'état de production opérationnel complet – ceci est dû à la fin mars 2011. La gestion des retouches des serveurs régionaux et des stations de

travail connectées directement aux serveurs est assurée par la Section des technologies de la sécurité nationale. La capacité d'assumer la gestion des retouches est améliorée par la Division de soutien des bureaux qui utilise un logiciel qui protège les postes de travail utilisateurs finaux en bloquant le trafic internet sujet à caution et en surveillant constamment les vulnérabilités du service de soutien afin d'empêcher les virus de se propager dans l'ordinateur et de s'étendre à tout le réseau. Santé Canada applique un solide cryptage et une norme unique d'authentification dans ses processus d'authentification et de gestion des justificatifs d'identité. L'accès aux services et aux outils du système est réservé au personnel administratif compétent des TI.

Il est également nécessaire d'effectuer régulièrement la gestion des retouches des stations de travail des utilisateurs finaux [redacted].

Gestion des comptes et services d'accès à distance : L'accessibilité aux biens de TI devrait être offerte en utilisant des connexions sécuritaires qui assurent la confidentialité, l'intégrité et l'authenticité du trafic entre le client et le réseau de Santé Canada. La section Fichiers, impression et accès à distance de la Division des services de bureautique est responsable des services « Web Office ». Le service utilise [redacted] pour assurer un réseau privé virtuel aux clients afin qu'ils accèdent au réseau du Ministère à l'aide de leur navigateur Web. Les utilisateurs peuvent accéder au réseau du Ministère par accès commuté et par Internet à haute vitesse. La Section de l'interconnectivité et des communications de la Division du centre des services des données gère ce processus.

Les sections Gestion à distance et Interconnectivité ont démontré qu'elles avaient appliqué des contrôles de sécurité et des mesures de protection efficaces au moment de mettre en œuvre leurs services d'accès à distance. Par exemple, l'utilisation d'un solide cryptage, l'adoption d'une norme unique d'authentification, des services ségrégés (privilèges d'accès) à l'intention du personnel administratif et de l'utilisateur final. Ces deux sections ont également démontré un niveau suffisant de redondance dans leur affectation des ressources de soutien et dans leur mise en œuvre d'une conception d'une grande disponibilité (reprise) dans leur architecture technique afin d'atténuer les risques d'un point unique de défaillance.

La Section gestion à distance est également responsable de la gestion des comptes utilisateurs [redacted].

[redacted]

[redacted].

2.4.2 Sécurité des TI et gestion du changement

Critère de vérification : *Les fonctions de gestion et les processus des IT ayant des composantes et des incidences sur la sécurité comme la gestion du changement et de la configuration, les comptes rendus des problèmes et la capacité de planification doivent être gérés conformément au profil de risques à la sécurité de Santé Canada.*

Selon la norme de GSTI, il est nécessaire d'obtenir un avis ou une approbation de la sécurité des TI dans le cadre du processus de gestion du changement où les changements pourraient éventuellement mettre le système à risque ou compromettre la sécurité. Étant une partie intégrante du processus et des pratiques de gestion du changement, le Comité consultatif sur le changement a été délégué par le dirigeant principal de l'information pour examiner régulièrement, valider et approuver ou rejeter par après une demande de changement lorsque la sécurité des TI est un facteur important.

La norme de GSTI exige que le Ministère possède un système de surveillance et une capacité de réseau afin de planifier et de mettre en œuvre des changements opportuns aux capacités. Un examen de dix demandes de changement a démontré que chacune de ces demandes concernait une menace à la sécurité. Elles ont été révisées et approuvées par la sécurité des TI et mises en œuvre conformément au processus de gestion du changement. Cependant, une fois les changements apportés, seulement 30 pour cent des demandes examinées ont été officiellement mises à l'essai pour s'assurer qu'elles fonctionnaient.

L'équipe de vérification a examiné les 42 demandes de changement rejetées par la sécurité des TI, ayant été jugées comme susceptibles d'entraîner un risque à la sécurité du réseau. L'examen a démontré que la sécurité des TI avait exercé la diligence requise en rejetant ces demandes.

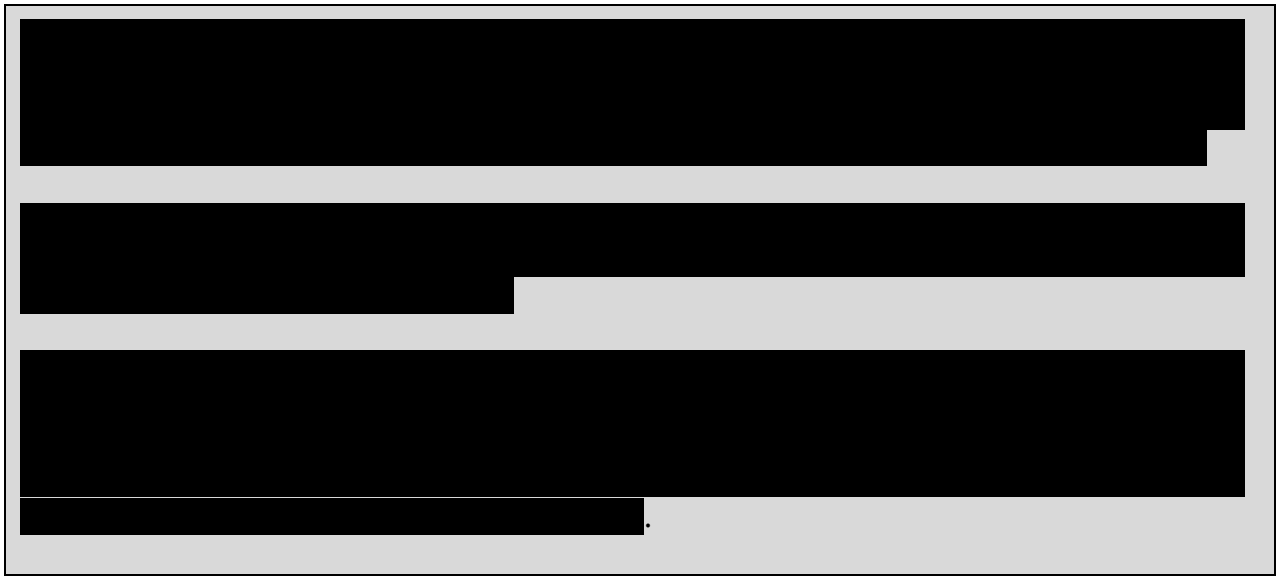
Recommandation 7

Il est recommandé au sous-ministre adjoint de la Direction générale des services de gestion, de renforcer les mesures de protection opérationnelles et techniques de la détection d'intrusion dans les stations de travail, la gestion des comptes, l'accès à distance et les demandes de gestion des changements.

Réponse de la direction

La direction souscrit à la recommandation.

[redacted]



2.4.3 Gestion des incidents

Critère de vérification : *Le Ministère devrait établir des mesures pour identifier et classer les incidents et imposer des sanctions qui s'imposent.*

Le Ministère devrait appliquer un processus pour identifier clairement les différentes sortes d'incidents et les clarifier en se basant sur une directive claire et précise et sur un processus d'évaluation des pratiques exemplaires. Il doit aussi appliquer un plan d'action précis sur la façon de traiter de tels incidents et de déterminer une intervention efficace lors d'incidents et des mécanismes de continuité des TI.

Cinq étapes à suivre pour traiter les incidents

1. Identification – déterminer la sorte, la sévérité et la cause d'un incident.
2. Intervention – déterminer la meilleure approche et prendre les mesures pour contrôler les dommages.
3. Rapport – communiquer les particularités de l'incident, y compris l'impact et l'intervention à SPCPC (Sécurité publique Canada et Protection civile) et à la gestion ministérielle.
4. Récupération – déterminer une approche pour rétablir et récupérer les systèmes et appliquer les changements à la sécurité approuvés aux dispositifs de sécurité (p. ex., les pare-feux et les règles de détection des incidents).
5. Analyse ultérieure – évaluer l'incident et recommander des changements aux processus et aux procédures si nécessaire.

De plus, la *Politique ministérielle sur la sécurité* exige des ministères qu'ils établissent des mécanismes pour intervenir avec efficacité lors d'incidents touchant les TI et de partager l'information liée aux incidents avec les principaux ministères en temps opportun.

La plupart des événements liés à la sécurité des TI sont reçus par l'intermédiaire du Centre de soutien technique national qui les transfert à la Boîte de services de la sécurité des TI . Chaque demande transmise au Soutien technique fait l'objet d'un suivi.

[redacted]. Actuellement, le Ministère met sur pied un plan de projet afin de se déplacer vers un processus de gestion d'incidents qui répond aux normes de la GSTI.

Intervention lors d'incidents de TI

Le Ministère devrait disposer d'un processus pour traiter l'inconduite ou la négligence envers la sécurité des TI, y compris des mesures pour déterminer, évaluer et préparer un rapport sur les incidents d'inconduite ou de négligence. Ce processus comprendrait aussi la détermination de mesures subséquentes nécessaires pour réduire ou minimiser à l'avenir les risques à la sécurité. De plus, le Ministère doit disposer d'une politique documentée concernant l'application de sanctions lorsque des incidents liés à la sécurité des TI sont dus à l'inconduite ou à la négligence.

La sécurité des TI comprend des fonctions antivirus et légistes comme celle du triage des incidents de TI suspects en milieu de travail. À la suite d'enquêtes, les rapports sont transmis aux parties demandeuses qui prendront les mesures nécessaires. En 2009, l'équipe légiste de la sécurité des TI a mené 147 enquêtes et a été impliquée dans 103 cas à ce jour. Habituellement, l'agent de sécurité ministériel a amorcé les enquêtes liées aux TI et a demandé de l'aide en se basant sur les allégations soulevées. Des directives ont été élaborées pour procurer un soutien fonctionnel à la gestion sur la façon de diriger une enquête administrative lorsqu'une allégation d'inconduite vise un employé ou un groupe d'employés.

Le rôle de l'agent de sécurité ministériel est de demeurer impartial à chaque enquête et à chaque rapport sur les constatations d'une enquête à la direction. Il appartient aux Relations de travail de recommander des mesures disciplinaires ou des sanctions qui seront appliquées par le gestionnaire.

Un programme de sécurité des TI serait le moyen idéal pour renforcer le processus de gestion des incidents et offrir à la direction l'application des sanctions (Voir la Recommandation 2).

3. Conclusion

Depuis 2006, Santé Canada s'est efforcé d'être à l'avant-garde de la gestion et de la technologie de l'information. D'importantes initiatives comme « Prochaines étapes » (2007-2008) ont mis l'accent sur la progression du Ministère vers de meilleures économies d'échelle et la normalisation dans la prestation de services en appliquant une approche aux TI. Durant cette époque, le Ministère a lancé le « Projet de conformité à la GSTI ». Le résultat le plus important a été l'élaboration de la *Politique ministérielle sur la sécurité des TI.* À la suite de ces importants résultats, Santé Canada a lancé plusieurs projets qui avaient pour objectif une évaluation de la capacité du Ministère à obtenir des produits d'information pour mener des évaluations des menaces et des risques des douze biens d'application les plus essentiels du Ministère. Au cours de cette période, une évaluation complète des menaces et des risques concernant l'interconnectivité du réseau a été réalisée en insistant sur les vulnérabilités de l'infrastructure du réseau des TI. Un important résultat attendu de ce projet a été un Plan d'application de mesures de protection (PAMP) ou une analyse des lacunes en décrivant où le Ministère était rendu et à quel endroit il devait être en ce qui a trait à la sécurité du réseau.

Même si beaucoup de choses ont été réalisées pour documenter les risques à la sécurité des TI, il y a encore beaucoup à accomplir pour atténuer les risques à la sécurité qui ont été décelés. Un programme intégré de sécurité des TI à l'appui des exigences de la *Politique sur la sécurité des TI* servira à traiter les risques à la sécurité et permettra au Ministère de progresser vers la conformité à la norme opérationnelle de sécurité. La réalisation de cette vérification de la sécurité des TI satisfait en soit les normes opérationnelles de sécurité. Ces normes stipulent que « les ministères et les organismes du gouvernement fédéral doivent évaluer et vérifier la sécurité des TI et corriger les déficiences si nécessaire » [TRADUCTION].

Santé Canada réalise encore des progrès pour trouver les lacunes dans les contrôles et l'endroit où il est nécessaire d'exercer des contrôles plus serrés et plus efficaces. La vérification a souligné qu'une organisation est bien en place et que des responsabilités pertinentes ont été déléguées pour gérer les activités et les risques de la sécurité du réseau des TI. Cependant dans les domaines des contrôles de la sécurité des TI et des mesures de protection techniques, il y a certains exemples où les contrôles et les mesures de protection ne sont pas vraiment efficaces, même s'ils font l'objet de nombreux contrôles.

Tout récemment, en novembre 2010, le Centre des services d'informatique et de réseau a proposé un « plan opérationnel » pour les cinq prochains exercices. Ce plan renferme des projets tels que [redacted], la transformation des services de soutien et un centre de protection de l'information. Bien que ce plan ne soit pas encore approuvé, ces projets sont en mesure de traiter certaines déficiences des contrôles identifiés dans la vérification et également de faire progresser le Ministère vers la conformité à la norme de sécurité opérationnelle.

Annexe A – Champs d'intérêt et critères

Critères
Organisation
Structure de gouvernance : Il doit y avoir un cadre de gouvernance pour assurer la surveillance de la sécurité des TI. **Rôles et responsabilités :** Des postes de gestionnaire principal définis dans la norme de sécurité opérationnelle doivent être confiés dans le Ministère.
Politique et programme
Politique de sécurité des TI : Il doit y avoir un politique de sécurité des TI appuyée par un programme de sécurité des TI.
Contrôles de la sécurité des TI
Gestion du cycle de vie des applications : Les contrôles de gestion de la sécurité des TI de Santé Canada doivent inclure tous les aspects du cycle de vie du développement d'un système.
Gestion des risques à la sécurité : Les ministères doivent gérer en permanence les risques à la sécurité de l'information et des biens des TI tout au long de la durée des programmes et des services.
Gestion de l'inventaire : La gestion de l'inventaire de l'information et des biens des TI doit être identifiée et classée par catégorie en retenant les caractéristiques qui soulignent la sensibilité, la criticité et autres qualités qui reflètent la valeur de l'organisation.
Gestion des vulnérabilités : Les vulnérabilités influençant l'infrastructure des TI de Santé Canada qui ont un impact sur les programmes, les systèmes et les services assurés par le Ministère doivent être continuellement évaluées.
Ségrégation du réseau : Le programme des TI devrait tenir compte de la ségrégation dans son architecture et sa stratégie de contrôles. La stratégie devrait comprendre la ségrégation des rôles, des responsabilités, des tâches, des objets, des processus, des accessoires et des fonctions afin d'atténuer les risques à l'infrastructure et aux systèmes des TI.
Mesures de protection opérationnelles et techniques
Stratégie de défense active : Santé Canada devrait adopter une stratégie de défense active comprenant la prévention la détection, l'intervention et la récupération.
Sécurité des TI et gestion du changement : Les fonctions opérationnelles et les processus de TI ayant une composante et une incidence sur la sécurité comme la gestion du changement et de la configuration, les rapports sur les problèmes et la capacité de planifier sont gérés conformément au profil de risques à la sécurité du Ministère.
Gestion des incidents : Le Ministère devrait appliquer des mesures pour identifier et classer par catégorie les incidents et les sanctions qui s'imposent.

Pages 21 à 22 exemptée en vertu des articles 16(2)(c), 21(1)(a), 21(1)(b) de la Loi sur l'accès à l'information