[*] Il y a un astérisque quand des renseignements sensibles ont été enlevés aux termes de la *Loi sur l'accès à l'Information* et de la *Loi sur la protection des renseignements personnels*.

BUREAU DU CONSEIL PRIVÉ

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

Division de la vérification et de l'évaluation

Rapport final

Le 16 novembre 2009

Table des matières

Sommaire

Objectif de la vérification

Cette vérification interne visait à évaluer le caractère adéquat de la sécurité des technologies de l'information (TI) afin de protéger les informations du Bureau du Conseil privé (BCP).

Portée

La vérification comportait une évaluation de la fonction de sécurité des TI au BCP, notamment sa gouvernance et son cadre stratégique; les procédures de gestion du risque et de la vulnérabilité; les processus de gestion des incidents, de la continuité opérationnelle, du développement des systèmes, des évaluations de sécurité, des contrôles opérationnels (accès aux réseaux et protection de ceux-ci) et de la sécurité physique; les ressources et la sensibilisation générale des employés.

La vérification n'a pas porté sur les évaluations techniques des mécanismes de contrôle tels que la surveillance du trafic sur les réseaux, les tentatives d'intrusion dans les réseaux ou la validation des paramètres du pare-feu. [*]

Conclusion de la vérification

Les progrès informatiques ont été rapides ces dernières années. Ils ont favorisé un plus haut niveau d'interconnexions ayant pour but de soutenir une prestation de services améliorée. Parallèlement à cela, il y a eu des hausses semblables du nombre et du potentiel de gravité de menaces et de sécurité informatiques. Dans un tel environnement, le BCP s'est doté d'une infrastructure de sécurité informatique évolutive, qui protège actuellement ses informations. Cependant, la vérification a permis de cerner des secteurs où des mesures doivent être prises par la direction afin de clarifier les rôles, de mieux planifier les mesures et les procédures de sécurité, et d'établir les ressources prioritaires, afin que le BCP puisse continuer de protéger efficacement ses informations.

Énoncé d'assurance

Selon mon opinion professionnelle, en ma qualité de dirigeant principal de la vérification, des procédures adéquates et suffisantes ont été mises en œuvre et des preuves ont été recueillies en appui des éléments sur lesquels se fonde la conclusion du rapport. Cette conclusion repose sur la comparaison des diverses conditions au moment de la vérification avec des critères préétablis avec la direction. Elle ne peut s'appliquer qu'à l'entité concernée. Les preuves ont été recueillies dans le respect des politiques, directives et normes du Conseil du Trésor en matière de vérification interne.

Résumé des conclusions et des recommandations

[*]

En ce qui concerne le régime global de sécurité des TI, la vérification a révélé des secteurs où des améliorations sont nécessaires pour respecter le Plan de continuité des activités (PCA). Le BCP a élaboré un cadre de gestion de continuité des activités, qui est en voie d'être mis en place. [*] Au niveau ministériel, la nécessité de renforcer la planification de la continuité des activités a été relevée dans le profil de risque de l'organisation, ainsi que dans une étude de cas de la Division des opérations de la sécurité.

L'environnement des TI au BCP étant exigeant, mais fondé sur la collaboration, il serait possible d'apporter des améliorations à moyen terme à la sécurité des TI, ce qui renforcerait les relations entre les intervenants responsables de la sécurité. Le cadre de gestion actuel de la sécurité des TI dépend largement [*]. Il faudrait mettre en place un programme viable de sécurité des TI impliquant tous les principaux intervenants pour mieux assurer la direction que les priorités sont prises en compte. De plus, la vérification a révélé que la consignation des procédures de collecte serait une façon de faire réaliste et souhaitable pour le transfert à long terme du savoir en matière de sécurité des TI.

Nos recommandations détaillées se trouvent dans le présent rapport. La direction s'est dite en accord avec toutes les recommandations et elle a préparé un plan de mise en œuvre de mesures correctives. Le plan d'action de la direction à cet égard figure à la section 3.0 du rapport.

Original signé par le Dirigeant principal de la vérification

SIGNATURE DU DIRIGEANT PRINCIPAL DE LA VÉRIFICATION
JIM HAMER

1.0 Introduction

1.1 Contexte

La Vérification de la sécurité des technologies de l'information a été approuvée dans le cadre du Plan de vérification interne pluriannuel (de 2008-2009 à 2010-2011) du Bureau du Conseil privé.

La vérification a été dirigée par la Division de la vérification et de l'évaluation (DVE) du BCP, qui a passé un marché avec Hallux Consulting Inc. La première étape de la planification s'est déroulée de février à mars 2009, et l'examen a été mené en avril et en mai 2009. La vérification fait suite aux travaux conduits par des vérificateurs de Finances Canada travaillant dans le cadre d'une entente de services partagés concernant la prestation de services de vérification interne au BCP avant que la DVE soit mise sur pied. En mai 2007, Finances Canada a soumis au Comité de vérification et d'évaluation du BCP un rapport sur l'examen préliminaire. [*]

Le BCP est régi par des politiques fédérales, notamment la Politique du gouvernement sur la sécurité (PGS) [1]. La PGS définit les exigences de base quant à la protection des employés et des biens, ainsi qu'à la prestation continue des services. En 2005, le Secrétariat du Conseil du Trésor (SCT) a demandé à tous les ministères – y compris au BCP – de mettre en oeuvre avant décembre 2006 les 144 normes contenues dans *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI)*. Les normes GSTI constituent l'exigence de base en ce qui touche les programmes ministériels de sécurité des TI et permettent aux ministères fédéraux, par exemple le BCP, d'assurer la sécurité de l'information et des composantes TI sous leur autorité. Elles donnent également des directives quant à la façon d'organiser les programmes, précisent les rôles et les responsabilités en matière de sécurité des TI ainsi que les mesures de protection techniques et opérationnelles conformes à la PGS sur la prévention, la détection, l'intervention et la reprise des activités.

Le SCT exige que les ministères et les organismes effectuent périodiquement des vérifications internes afin d'évaluer leur niveau de conformité à la PGS et si cette dernière est efficacement mise en application.

1.2 Objectif

Cette vérification interne visait à évaluer le caractère adéquat de la sécurité des technologies de l'information (TI) afin de protéger les informations du BCP.

[1] Le 1er juillet 2009, la Politique sur la sécurité du gouvernement du Conseil du Trésor a remplacé la Politique sur la sécurité.

1.3 Portée

La vérification comportait une évaluation de la fonction de sécurité des TI au BCP, notamment sa gouvernance et son cadre stratégique; les procédures de gestion du risque et de la vulnérabilité; les processus de gestion des incidents, de la continuité opérationnelle, du développement des systèmes, des évaluations de sécurité, des contrôles opérationnels (accès aux réseaux et protection de ceux-ci) et de la sécurité physique; les ressources et la sensibilisation générale des employés.

La vérification n'a pas porté sur les évaluations techniques des mécanismes de contrôle tels que la surveillance du trafic sur les réseaux, les tentatives d'intrusion dans les réseaux ou la validation des paramètres du pare-feu. [*]

1.4 Approche et méthodologie

Pour évaluer la conformité aux GSTI, une approche générique a été utilisée par l'équipe de vérification. Les normes GSTI ont été harmonisées aux quatre volets du Cadre de responsabilisation de gestion (CRG) du SCT, c'est-à-dire la responsabilisation, la gestion du risque, la gérance et les personnes. Les critères de vérification se trouvent à l'Annexe A.

2.0 Observations, conclusions et recommandations

Aux fins de cette vérification interne, le rapport se divise en trois grands thèmes touchant la sécurité des TI au BCP : 1) améliorations immédiates touchant la sécurité; 2) programme en matière de sécurité des TI; 3) procédures officielles en sécurité des TI. Étant donné que la sécurité des TI englobe de nombreux éléments, la vérification a généré plusieurs observations, certaines positives et d'autres nécessitant que des mesures soient prises par la direction. Les rubriques suivantes expliquent en détail les observations, conclusions et recommandations de l'équipe de vérification.

2.1 Améliorations immédiates touchant la sécurité

Concernant le régime global de sécurité des TI, la vérification a révélé que des améliorations, nécessaires et réalistes à court terme, devaient être apportées dans certains secteurs. Les vérificateurs s'attendaient à trouver : un programme normalisé de pratiques exemplaires en matière de sécurité des installations et des systèmes; un programme efficace, bien documenté et bien exécuté de sécurité et de protection des réseaux; un cadre de gestion de la continuité des activités (GCA) composé d'une structure de gouvernance ainsi que d'un plan de continuité des activités de TI, et d'un plan de reprise après sinistre en technologies de l'information bien documentés, à jour et testés.

Sécurité physique et supports TI

[*] La vérification a permis de constater que [*]. De plus, du personnel chargé de la sécurité est positionné aux entrées stratégiques. Les procédures et les processus en place quant à la protection, à la consignation, au transport et à l'élimination des supports de sauvegarde sont conformes à la GSTI et aux pratiques exemplaires.

[*] mais l'accès à la salle est bien contrôlé. Dans cette salle, l'équipement est correctement marqué, [*]. La Division de l'informatique et des services techniques (DIST), Direction des services ministériels, travaillent actuellement à rationaliser l'équipement dans le but d'accroître l'efficacité et réduire les coûts. [*]

Sécurité des réseaux

Bien que la sécurité physique soit un élément clé et représente la première ligne de défense pour ce qui touche l'environnement de sécurité des TI, les mesures de protection des réseaux sont une combinaison d'équipement, d'outils logiciels et de fonctions nécessaires exercées par des experts. [*]

Continuité des activités

La protection des réseaux de TI par des mesures physiques et autres garantit la prestation continue des services. De plus, [*]. Un PRSTI valide (à jour et mis à l'essai) constitue un outil de gestion clé pour atténuer les risques découlant d'une vulnérabilité;

il constitue un élément essentiel de la stratégie de continuité des activités de toute organisation.

[*]

Conclusion

[*]

Recommandation

1. Sous-ministre adjoint, Direction des services ministériels :
[*]

2.2 Programme de sécurité des TI

L'environnement des TI au BCP étant complexe, mais fondé sur la collaboration, il serait possible d'apporter des améliorations à moyen terme à la sécurité des TI. Les vérificateurs s'attendaient à trouver un programme exhaustif de sécurité des TI dirigé par un professionnel de la sécurité des TI qualifié et d'expérience à titre de coordonnateur de la sécurité des TI (CSTI). Ils ont également cherché à vérifier si l'intention et l'orientation de la PGS et de la GSTI étaient manifestes dans les rôles clés, y compris celui du Agent de sécurité du ministère (ASM), du Dirigeant principal de l'information (DPI), du coordonnateur de la PCA et du CSTI, ainsi que dans la structure de gestion de la sécurité.

<u>Gouvernance</u>

La vérification a révélé qu'il existe une bonne relation de travail entre les principaux intervenants en matière de sécurité, un fait que tous les participants ont approuvé. Une discussion sur les rôles et les responsabilités en sécurité est [*] au BCP. Le rôle de CSTI est attribué au chef, sécurité des TI, qui relève du directeur exécutif de la DIST, Direction des services ministériels. Le CSTI [*] pour garantir une application efficace du programme de sécurité des TI au BCP. [*]

La gestion de la sécurité des TI exige la collaboration de l'ASM, du CSTI et du DPI. Le directeur exécutif de la DIST assume le rôle de DPI, comme le prévoit la description de poste, mais ce rôle n'est pas prévu dans la Politique de sécurité du BCP. La Division des services d'information ministériels (DSIM), Direction des services ministériels, s'occupe de la gestion de l'information (GI) au BCP. [*]

La DIST a fait des progrès pour ce qui est de documenter les exigences en gestion de projets de TI, et leurs répercussions sur la sécurité des TI. Par exemple, les mécanismes de contrôle en gestion des projets de TI ont été améliorés par la création, tout récemment, du Comité de gestion des solutions commerciales (CGSC) au sein de la DIST, et de l'élaboration connexe de documents sur la gestion et le déploiement des projets. [*] La vérification souligne que [*] à l'heure actuelle. [*]

Politique

Chaque ministère fédéral doit se doter d'une politique de sécurité des TI pour respecter la PGS et les normes GSTI. Le BCP a une politique [*] qui repose à la fois sur des politiques, des procédures et des lignes directrices. [*]

Planification du programme de sécurité

Le financement continu de la sécurité est établi dans le cadre du cycle budgétaire annuel du BCP. Des fonds sont ensuite affectés à la sécurité des TI au niveau opérationnel, notamment aux fins d'exigences en matière de sécurité des TI de grands projets. D'autre part, [*]

Les gestionnaires et les employés du BCP sont en général conscients du caractère sensible de l'information et des conventions quotidiennes à suivre pour réduire les risques sur le plan de la sécurité de l'information. Une approche à la sensibilisation en matière de sécurité fondée sur des règles existe; [*]. Il faut continuer d'offrir de la formation sur la sécurité aux employés du BCP afin de les aider à maintenir un haut niveau de compréhension des exigences en matière de politiques sur la sécurité et à comprendre comment travailler en tenant compte des protocoles de sécurité existants. [*]

Conclusion

[*]

Recommandations

2. ***Que le sous-ministre adjoint, Direction des services ministériels, en collaboration avec le sous-secrétaire du Cabinet, Politique étrangère et défense,*** [*]

3. ***Que le sous-secrétaire du Cabinet, Politique étrangère et défense, continue d'offrir de la formation sur la sécurité aux employés du BCP afin de les aider à maintenir un haut niveau de compréhension des exigences en matière de politiques sur la sécurité et à comprendre comment travailler en tenant compte des protocoles de sécurité existants.***

2.3 Procédures officielles en matière de sécurité des TI

Documenter les procédures et les processus représente un objectif réalisable et souhaitable pour le transfert à long terme des connaissances en TI. Les vérificateurs s'attendaient à trouver un ensemble de procédures en matière de TI et de sécurité des TI conformes aux prescriptions de la GSTI, y compris : un programme structuré de gestion des risques et d'évaluation des vulnérabilités; un processus structuré de gestion

des incidents; une série normalisée de pratiques exemplaires aux fins du cycle chronologique de l'élaboration des systèmes, ainsi que la gestion et les techniques connexes; un programme de vérification et d'évaluation de la sécurité des TI ainsi qu'un processus normalisé opérationnel de gestion de l'accès; des pratiques exemplaires dans la gestion des clés et de l'équipement cryptographiques.

Gestion des risques

La gestion des risques s'accomplit dans le cadre de la gestion des projets et de l'examen du budget. L'analyse du budget de fonctionnement des TI s'inscrit dans le cycle des projets et des initiatives en matière de sécurité, et s'effectue annuellement (au minimum) ou selon les besoins. Une série de pratiques de gestion des risques a été établie [*] tous les ans ou aux deux ans pour [*]. Le personnel des TI et de la sécurité du BCP est conscient des enjeux de sécurité propres au milieu du BCP. [*]

Gestion des incidents

Les incidents sont gérés de manière [*].

Certification et accréditation

Le processus de sécurité des TI fait partie intégrante du cycle chronologique de l'élaboration des systèmes dont l'un des éléments consiste à certifier et à accréditer les logiciels qui seront utilisés sur les réseaux du BCP. La documentation de la DIST décrit son rôle à l'égard du soutien et de la maintenance des progiciels. [*]

Accès et cryptage

La nature du contrôle de l'accès et du cryptage en fait des éléments indispensables pour garantir la confidentialité et l'intégrité de l'environnement des TI. L'un et l'autre élément doit fonctionner aux niveaux voulus pour que la protection soit assurée. [*] et les comptes désuets sont supprimés ou désactivés sur demande. Le cryptage et les activités connexes répondent [*].

Vérification et évaluation

Des autoévaluations sont effectuées conformément à la GSTI et sont correctement documentées. [*]

Conclusion

[*]

Recommandation

4. ***Que le sous-ministre adjoint, Direction des services ministériels, veille à ce que*** [*]

3.0 Réponse et plan d'action de la direction

Vérification de la sécurité des TI
La responsabilité générale du plan d'action relève du sous-ministre adjoint, Direction des services ministériels, et du sous-secrétaire du Cabinet, Politique étrangère et défense.

Recommandation	Mesures de suivi	Responsabilité	Date cible
1. Que le sous-ministre adjoint, Direction des services ministériels : [*]	La direction accepte la recommandation. [*]	Sous-ministre adjoint, Direction des services ministériels	Novembre 2009
[*]	La direction accepte la recommandation. [*]	DPI	Janvier 2011
2. Que le sous-ministre adjoint, Direction des services ministériels, en collaboration avec le sous-secrétaire du Cabinet, Politique étrangère et défense, [*]	La direction est d'accord avec la recommandation. La direction s'assurera que : [*]	DPS DPI	a) Mai 2010 b) Janvier 2010
[*]	La direction appuie la recommandation. [*]	DPS et DPI	
[*]	La direction appuie la recommandation. [*]	DPS et DPI	Mai 2010
[*]	La direction appuie la recommandation. [*]	DPS et DPI	Août 2009

Recommandation	Mesures de suivi	Responsabilité	Date cible
3. Que le sous-secrétaire du Cabinet, Politique étrangère et défense, continue d'offrir de la formation sur la sécurité aux employés du BCP afin de les aider à maintenir un haut niveau de compréhension des exigences en matière de politiques sur la sécurité et à comprendre comment travailler en tenant compte des protocoles de sécurité existants.	La direction appuie cette recommandation. • On a élaboré des séances de formation et de sensibilisation pour aider les employés à bien marquer les documents classifiés, ainsi qu'à bien les transmettre et les détruire.	Dirigeant de la sécurité	En permanence
4. Que le sous-ministre adjoint, Direction des services ministériels, veille à ce que [*]	La direction appuie cette recommandation. [*]	Directeur adjoint, Sécurité des technologies de l'information	Mars 2010
[*]	La direction appuie cette recommandation. [*]	Directeur adjoint, Sécurité des technologies de l'information	Mars 2010
[*]	La direction appuie cette recommandation. [*]	Directeur adjoint, Sécurité des technologies de l'information et Directeur adjoint, Gestion des solutions commerciales	Juin 2011
[*]	[*]	Directeur adjoint, Sécurité des technologies de l'information	Juin 2011

Annexe A : Critères de vérification

Élément du Cadre de responsabilisation de gestion (CRG) du SCT	Élément de la GSTI
Responsabilisation. Les responsabilités en ce qui concerne les résultats sont clairement attribuées et correspondent aux ressources et les délégations tiennent compte des capacités. Mots clés : liens hiérarchiques et responsabilités clairs, enchaînement des engagements, ententes de gestion du rendement.	**Organisation (gouvernance).** Une division de la sécurité bien organisée définit clairement les rôles, les responsabilités ainsi que l'interaction de la haute direction, des gestionnaires des risques, des directeurs de programme, des spécialistes de la sécurité et des employés chargés de la sécurité des TI. Un programme efficace en matière de sécurité des TI assure une bonne attribution des tâches parmi les intervenants, une compréhension commune des responsabilités de sécurité, et favorise un haut niveau d'interaction.
	Politique. En vue de garantir le respect des exigences de la PGS et de la GSTI, tous les ministères/ organismes doivent appliquer une politique en matière de sécurité des TI, adaptée à leur secteur d'activités, et définir leurs obligations premières.
Gestion des risques. L'équipe de la haute direction définit clairement le contexte ministériel et les pratiques de gestion proactive des risques organisationnels et stratégiques. Mots clés : définition des risques clés, prise en compte des risques dans le processus décisionnel, culture consciente des risques.	**Gestion des risques.** La gestion des risques est essentielle pour garantir l'efficacité d'un programme de sécurité des TI. Les spécialistes de la sécurité des TI doivent gérer les risques de façon continue, car les menaces et l'environnement opérationnel évoluent constamment. La haute direction, les gestionnaires des risques, les directeurs de programme et les spécialistes de la sécurité ont tous un rôle à jouer quant à la gestion et à l'intégration de la sécurité des TI dans le profil de risque global de l'organisation. Un programme rigoureux de gestion des risques prend en compte les menaces, les vulnérabilités, les répercussions, les probabilités et les mesures de sécurité.
	Gestion des vulnérabilités. Les vulnérabilités peuvent survenir à tout moment lors de la conception ou de la mise en opération d'un système des TI. Une fois qu'elles sont cernées, les risques qui y sont associés doivent être atténués ou acceptés.
	Détermination du matériel de TI. La détermination du matériel de TI essentiel est nécessaire à l'établissement des priorités organisationnelles, à la protection des services essentiels les plus importants ainsi qu'à l'atténuation des risques de sécurité suivant leur importance.

Élément du Cadre de responsabilisation de gestion (CRG) du SCT	Élément de la GSTI
Gérance. Le régime de contrôle ministériel (actif, fonds, effectifs, services, etc.) est intégré et efficace et tous les employés comprennent bien ses principes sous-jacents. Mots clés : information pertinente produite par les systèmes, fonction de vérification, respect des lois, politiques et règlements.	**Gestion des incidents.** En matière de sécurité des TI, les incidents qui impliquent l'accès à un système, sa modification, sa perturbation ou sa mise en échec pourraient avoir d'importantes répercussions sur la prestation des programmes et des services. À l'instar de la gestion des vulnérabilités, les ministères/ organismes doivent faire preuve de vigilance pour ce qui est de la recherche, de la détection et de la gestion des incidents.
	Planification de la continuité. La planification de la continuité des activités, qui comprend la gestion de l'information (GI) et la planification de la continuité des TI, garantit la disponibilité des ressources nécessaires au maintien des activités du gouvernement.
	Cycle chronologique de l'élaboration des systèmes (CCES). Il est plus simple, plus rentable et plus sûr de mettre en place des mécanismes de sécurité en matière de TI au moment de l'élaboration et de la mise en œuvre d'un programme ou d'un service plutôt qu'après son implantation.
	Évaluation et vérification. L'examen annuel de la sécurité permet aux membres de la haute direction d'être informés des problèmes touchant les activités de l'organisation et de prendre les mesures qui s'imposent. L'examen est effectué au moyen d'outils d'évaluation du rendement, notamment des outils d'autoévaluation et des vérifications externes.
	Contrôles opérationnels. – sécurité matérielle et systèmes de TI – contrôle de l'accès et cryptage – protection des réseaux.
Personnes. Le ministère possède les effectifs et le milieu de travail voulu et met l'accent sur l'acquisition des compétences pour assurer son succès et un excellent avenir pour la fonction publique du Canada. Mots clés : capacité renouvelée/continue, milieu de travail positif, leadership.	**Ressources.** La création et l'élargissement de programmes et de services nécessitent l'allocation adéquate de ressources pour garantir le respect des exigences en matière de sécurité des TI. Les ressources requises doivent être définies dans le processus de planification des activités; la disponibilité insuffisante de ressources humaines qualifiées et un financement inadéquat représentent une entrave majeure au respect de la GSTI.
	Communication. Les ministères doivent informer régulièrement le personnel de leurs rôles et responsabilités en matière de sécurité des TI. La communication est nécessaire pour améliorer la connaissance des risques touchant la sécurité des TI et combler l'écart entre les dirigeants d'entreprise et la collectivité de la sécurité des TI.

Annexe B : Liste d'acronymes

Agent de sécurité du ministère	ASM
Cadre de responsabilisation de gestion	CRG
Centre de la sécurité des télécommunications	CSTC
Comité de gestion des solutions commerciales	CGSC
Comité de vérification et d'évaluation	CVE
Coordonnateur de la sécurité des technologies de l'information	CSTI
Dirigeant principal de l'information	DPI
Division de l'informatique et des services techniques	DIST
Division des services d'information ministériels	DSIM
Évaluation de la menace et des risques	EMR
Évaluation des vulnérabilités	EV
Gestion de l'information	GI
Gestion de la continuité des activités	GCA
Gestion de la sécurité des technologies de l'information	GSTI
Gestion des risques	GR
Planification de la continuité des activités	PCA
Plan de reprise après sinistre en technologies de l'information	PRSTI
Politique du gouvernement sur la sécurité	PGS
Sécurité des communications	COMSEC