Travaux publics et Services gouvernementaux Canada

Public Works and Government Services Canada

Canada

Respect ♦ Intégrité ♦ Excellence ♦ Leadership

Au service du GOUVERNEMENT, au service des CANADIENS.

Rapport Final

2009-714
Vérification de la conformité de TPSGC a certaines exigences de la norme de Gestion de la sécurité des technologies de l'information

Le 8 septembre 2011

Bureau de la vérification et de l'évaluation

www.tpsgc-pwgsc.gc.ca

TABLE DES MATIÈRES

POINTS SAILLANTS

Objet

i. La *Politique du gouvernement sur la sécurité* de 2002 (remplacée en 2009 par la *Politique sur la sécurité du gouvernement*) définit les exigences de base en matière de protection des employés et des biens, et de prestation continue des services. Le Secrétariat du Conseil du Trésor du Canada a renforcé cette politique en établissant des directives en matière de sécurité et des normes opérationnelles de sécurité. Une de ces normes, la Gestion de la sécurité des technologies de l'information (GSTI), entrée en vigueur en 2004, exige que le Ministère s'y conforme entièrement avant le 31 décembre 2006.

ii. La présente vérification portait sur la conformité aux éléments de la norme de GSTI considérés par le Bureau de la vérification et de l'évaluation comme présentant un risque élevé pour le Ministère. Plus précisément, nous avons examiné la conformité de certaines portions de six systèmes de technologie de l'information (TI) essentiels de la région de la capitale nationale qui soutiennent des services essentiels. Les systèmes sélectionnés pour la présente vérification sont les suivants : le Système de gestion des projets et des activités, la solution SIGMA (le système de gestion financière et de gestion du matériel de TPSGC), le système de production de la Gazette du Canada, le logiciel LDRPS (système évolutif de planification de la reprise du traitement après sinistre),le Système de gestion des documents et de l'information de l'entreprise et le Système d'information sur la sécurité ministérielle et industrielle.

iii. Même si la vérification était exclusivement axée sur les systèmes susmentionnés, nous prévoyons que les résultats de la présente vérification serviront à améliorer la sécurité de tous les systèmes de TI du Ministère. Par conséquent, nous nous attendons à ce que l'étendue des mesures incluses dans le Plan d'action de la gestion établies en réponse aux recommandations formulées à la suite de la vérification englobe tous les systèmes de TI essentiels et non seulement les six systèmes examinés dans le cadre la vérification.

Importance

iv. La sécurité des TI fait partie intégrante de la prestation continue de programmes et de services. Une protection adéquate des TI peut prévenir les interruptions de service que pourraient causer les atteintes à la sécurité des TI. La norme de GSTI définit les exigences sécuritaires de base auxquelles les ministères fédéraux doivent satisfaire pour assurer la sécurité de l'information et des biens de TI placés sous leur contrôle.

v. En mars 2005, le Bureau du vérificateur général (BVG) a exprimé des préoccupations au sujet de la sécurité des TI au sein du gouvernement fédéral. Le BVG a indiqué que la haute direction ne connaît pas les risques associés à la sécurité des TI et ne comprend pas comment une atteinte à la sécurité des TI pourrait avoir des répercussions sur les activités et la crédibilité du gouvernement. Le BVG a également déclaré que la majorité des ministères ne répondent pas aux normes minimales de sécurité des TI. En octobre 2005, le Secrétariat

du Conseil du Trésor (SCT) a déclaré que la norme de GSTI est essentielle aux efforts du gouvernement du Canada pour améliorer la sécurité des TI.

vi. En 2005 et en 2006, les ministères ont dû soumettre au SCT un rapport d'auto-évaluation sur leur conformité à la norme de GSTI. Par la suite, le SCT a intégré ces auto-évaluations au Cadre de responsabilisation de gestion (CRG).

Constatations

vii. Nous avons constaté que la vulnérabilité de l'infrastructure des systèmes de TI essentiels accessible de l'extérieur du réseau de TPSGC avait été évaluée sur une base régulière. L'évaluation de la vulnérabilité des éléments des systèmes de TI essentiels accessibles de l'intérieur de TPSGC n'étaient effectuées que si l'administrateur du système de TI essentiel faisait la demande expresse et n'étaient pas effectuées sur une base régulière. Cinq des six systèmes essentiels sélectionnés dans le cadre de la présente vérification n'étaient accessibles que par le biais du réseau interne de TPSGC. Nous avons également observé qu'aucune procédure officielle n'avait été mise en place pour s'assurer que des mesures étaient prises afin d'atténuer les vulnérabilités identifiées et de surveiller la mise en œuvre de telles mesures.

viii. Toutefois, nous avons constaté que quatre des six systèmes de TI essentiels sélectionnés étaient dotés d'un processus de gestion des correctifs approuvés qui permet de s'assurer que les correctifs de sécurité sont installés en temps opportun.

ix. Nous avons constaté que cinq des six systèmes de TI essentiels vérifiés faisaient l'objet d'une séparation des tâches appropriée pour prévenir des modifications non autorisées aux systèmes, aux bases de données ou aux serveurs.

x. Enfin, nous avons constaté que des journaux de vérification de sécurité avaient été produits et examinés pour quatre des six systèmes de TI essentiels vérifiés.

Réponse de la gestion

La Direction générale des services d'infotechnologie (DGSIT) a examiné le rapport de vérification et accepte les recommandations qui y figurent. La DGSIT a élaboré un plan d'action de la gestion pour s'assurer que les recommandations de la vérification soient appliquées adéquatement.

La direction prend acte des conclusions du rapport de vérification et désire souligner que la DGSIT considère que le rapport Continuité opérationnelle et exigences essentielles en matière de TI (COEETI) 2010 de TPSGC constitue le registre définitif des systèmes essentiels du Ministère. La direction a déjà répondu à plusieurs des recommandations incluses dans le rapport de vérification. Par exemple, la DGSIT a procédé à l'achèvement de l'évaluation de la vulnérabilité de la COEETI afin de cerner les dépendances clés entre les services critiques et les systèmes de TI. La direction a également augmenté le nombre d'évaluations de la vulnérabilité effectuées sur

les interfaces externes et a amélioré les processus de surveillance des vulnérabilités découvertes au cours des évaluations et de mise en application de mesures correctives. Enfin, le Système d'information sur la sécurité ministérielle et industrielle (SISMI) a été transféré dans un centre de données géré par la DGSIT et est désormais pris en charge avec la même rigueur que les autres systèmes essentiels.

Recommandation 1 : Le Dirigeant principal de l'information, Direction générale des services d'infotechnologie, devrait mettre en place des mécanismes permettant d'assurer que tous les systèmes de TI très délicats ou assortis de risques importants qui sont soutenus par la DGSIT soient soumis de façon régulière à des évaluations de la vulnérabilité, et que les vulnérabilités identifiées fassent l'objet d'un suivi formel et soient corrigées.

> **Plan d'action de la gestion 1.1 :** Définir une norme d'évaluation de la vulnérabilité, notamment un calendrier d'examens continus de tous les systèmes de TI de niveau 1 et de tous les systèmes de TI très délicats ou assortis de risques importants de TPSGC qui sont appuyés par la DGSIT.
>
> **Plan d'action de la gestion 1.2 :** Cerner les lacunes et examiner le processus afin de satisfaire à la norme définie au point 1.1.
>
> **Plan d'action de la gestion 1.3 :** Mettre en œuvre le processus et préciser les exigences nécessaires en matière de mesures correctives afin de satisfaire à la norme d'évaluation de la vulnérabilité définie au point 1.1
>
> **Plan d'action de la gestion 1.4 :** À compter de mars 2012, produire régulièrement des rapports sur la conformité pour le Coordonnateur de la sécurité de la TI. Les rapports porteront sur les activités définies pour combler les lacunes d'un statut non conforme.

Recommandation 2 : Le Dirigeant principal de l'information, Direction générale des services d'infotechnologie, devrait examiner le processus de gestion des correctifs pour tous les systèmes de TI essentiels qui sont soutenus par la DGSIT et travailler en collaboration avec les sous-ministres adjoints responsables afin d'assurer que des correctifs appropriés soient apportés aux systèmes.

> **Plan d'action de la gestion 2.1 :** Définir une norme de gestion des correctifs, notamment un calendrier d'examens continus de tous les systèmes de TI de niveau 1 et de tous les systèmes de TI très délicats ou assortis de risques importants de TPSGC qui sont appuyés par la DGSIT.
>
> **Plan d'action de la gestion 2.2 :** Cerner les lacunes en fonction de la norme définie au point 2.1.
>
> **Plan d'action de la gestion 2.3** : Déterminer les mesures correctives nécessaires pour satisfaire à la norme.

Plan d'action de la gestion 2.4 : À compter de mars 2012, produire régulièrement des rapports sur la conformité pour le Coordonnateur de la sécurité de la TI. Les rapports porteront sur les activités définies pour combler les lacunes d'un statut non conforme.

Recommandation 3 : Le Dirigeant principal de l'information, Direction générale des services d'infotechnologie, devrait examiner la séparation des tâches pour tous les systèmes de TI essentiels qui sont soutenus par la DGSIT et travailler en collaboration avec les sous-ministres adjoints responsables pour répondre aux préoccupations soulevées au sujet des responsabilités conflictuelles.

Plan d'action de la gestion 3.1 : Définir une norme de séparation des tâches, notamment un calendrier d'examens continus de tous les systèmes de TI de niveau 1 et de tous les systèmes de TI très délicats ou assortis de risques importants de TPSGC qui sont appuyés par la DGSIT.

Plan d'action de la gestion 3.2 : Cerner les lacunes en fonction de la norme définie au point 3.1.

Plan d'action de la gestion 3.3 : Déterminer les mesures correctives nécessaires pour satisfaire à la norme.

Plan d'action de la gestion 3.4 : À compter de mars 2012, produire régulièrement des rapports sur la conformité pour le Coordonnateur de la sécurité de la TI. Les rapports porteront sur les activités définies pour combler les lacunes d'un statut non conforme.

Recommandation 4 : Le Dirigeant principal de l'information, Direction générale des services d'infotechnologie, devrait examiner les fonctions de journal de vérification de sécurité de tous les systèmes de TI essentiels qui sont soutenus par la DGSIT et travailler en collaboration avec les sous-ministres adjoints responsables afin de combler les lacunes identifiées pour le logiciel LDRPS et le Système d'information sur la sécurité ministérielle et industrielle (SISMI).

Plan d'action de la gestion 4.1 : Définir une norme de surveillance des registres de contrôle de la sécurité, notamment un calendrier d'examens continus de tous les systèmes de TI de niveau 1 et de tous les systèmes de TI très délicats ou assortis de risques importants de TPSGC qui sont appuyés par la DGSIT.

Plan d'action de la gestion 4.2 : Cerner les lacunes en fonction de la norme définie au point 4.1.

Plan d'action de la gestion 4.3 : Déterminer les mesures correctives nécessaires pour satisfaire à la norme.

Plan d'action de la gestion 4.4 : À compter de mars 2012, produire régulièrement des rapports sur la conformité par rapport à la norme pour le Coordonnateur de la sécurité de la TI. Les rapports porteront sur les activités définies pour combler les lacunes d'un statut non conforme.

Recommandation 5 : Conformément aux exigences de la Politique sur la sécurité des technologies de l'information (PM 104), le Dirigeant principal de l'information, Direction générale des services d'infotechnologie, devrait fournir des conseils techniques aux sous-ministres adjoints afin d'assurer la sécurité de tous les systèmes ministériels de TI qui ne sont pas soutenus par la DGSIT, y compris des conseils pour faire en sorte que les exigences en matière d'évaluation de la vulnérabilité, de gestion des correctifs, de séparation des tâches et de journal de vérification de sécurité soient respectées.

Plan d'action de la gestion 5.1 : Fournir une orientation fonctionnelle aux SMA et aux DGR en informant le Comité ministériel sur la sécurité des responsabilités des régions et des directions générales en matière de GSTI.

Plan d'action de la gestion 5.2 : Transmettre les normes de TPSGC (précisées aux points 1.1, 2.1, 3.1 et 4.1), aux SMA et DGR concernés pour tous les systèmes de TI de niveau 1 et de tous les systèmes de TI très délicats ou assortis de risques importants de TPSGC qui ne sont pas appuyés par la DGSIT et demander qu'ils respectent ces normes.

Plan d'action de la gestion 5.3 : Demander aux SMA et aux DGR concernés de contrôler et de confirmer la conformité par rapport aux normes de TPSGC (définies aux points 1.1, 2.1, 3.1 et 4.1) et de faire rapport au Coordonnateur de la sécurité de la TI. Les rapports incluent les activités définies pour combler les lacunes d'un statut non conforme.

Plan d'action de la gestion 5.4 : À compter de mars 2012, contrôler et signaler régulièrement les plans d'action énumérés au point 5.3 au DPI.

INTRODUCTION

1. La *Politique sur la sécurité du gouvernement* énonce les exigences à respecter pour protéger les biens du gouvernement, y compris l'information, et prescrit aux ministères et organismes fédéraux touchés par cette politique de se doter d'une stratégie de sécurité en matière de technologies de l'information. La *Politique sur la gestion de l'information* exige des ministères qu'ils traitent l'information et les documents comme des biens de grande valeur. La norme de *Gestion de la sécurité des technologies de l'information (GSTI)* s'attarde aux exigences de ces deux politiques.

2. La norme de GSTI définit les exigences de base en matière de sécurité que les ministères fédéraux doivent satisfaire. Ces exigences comprennent des éléments tels que la gestion de la vulnérabilité des programmes, des systèmes et des services; la détermination des menaces et la mise en œuvre de solutions adéquates; la gestion des correctifs, notamment l'acquisition, les essais et l'installation de correctifs pour les logiciels; la séparation des tâches et la tenue d'un journal de vérification de sécurité dans lequel on consigne les activités liées à la sécurité, à l'intégrité et à la disponibilité d'un système. La norme de GSTI appuie une philosophie de gestion des risques selon laquelle la mise en œuvre des exigences de base et de mesures de protection supplémentaires devrait être déterminée au moyen d'une approche fondée sur le risque.

3. Aux fins de la norme de GSTI, le terme « sécurité des TI » se définit comme les mesures de protection visant à préserver la confidentialité, l'intégrité, la disponibilité, l'utilisation prévue et la valeur des renseignements conservés, traités ou transmis par voie électronique.

4. Les gestionnaires responsables de la prestation des programmes et des services peuvent déléguer la responsabilité de la sécurité des TI à des experts techniques; cependant, ils demeurent redevables envers les administrateurs généraux et sont responsables d'assurer la sécurité des programmes et des services placés sous leur autorité. À TPSGC, la responsabilité de la mise en œuvre de la sécurité des TI a été déléguée au directeur, Direction de la sécurité de la technologie de l'information (DSTI), qui relève de la Direction générale des services d'infotechnologie (DGSIT). D'autres secteurs de la DGSIT sont également touchés par la norme de GSTI.

5. La *Politique sur la sécurité des technologies de l'information de TPSGC (PM 104)*, publiée en juillet 2010, assure la sécurité des renseignements électroniques de TPSGC, de ses biens de TI et de ses services connexes. Elle permet de s'assurer que tous les intervenants clés interpréteront de la même manière leur rôle, leurs responsabilités et leurs obligations relativement à la sécurité des TI. Elle vient appuyer le Programme de sécurité de la TI du Ministère, et devrait être lue conjointement avec la norme de GSTI. Conformément à cette politique, la responsabilité générale du programme ministériel de la sécurité de la TI incombe à la DGSIT, tandis que les chefs de direction générale sont responsables de fournir et

d'assurer un financement suffisant pour vérifier périodiquement et fréquemment si les exigences en matière de sécurité des systèmes de TI sont respectées.

6. La DGSIT fournit du soutien à la gestion de l'information (GI)/technologie de l'information (TI) pour environ 80 % des systèmes de TI à TPSGC. La DGSIT ne possède pas, n'exploite pas et ne soutient pas tous les systèmes de TI du Ministère, car certaines directions générales choisissent de développer et d'exploiter leurs propres systèmes, indépendamment de la DGSIT. Deux secteurs de la DGSIT sont responsables de l'exploitation et des services relatifs aux TI. Les Services de gestion des applications et services opérationnels de technologie de l'information (SGASOTI) assurent le soutien opérationnel des applications et de l'infrastructure pour TPSGC. L'infrastructure de TI comme telle est obtenue auprès du Secteur de la gestion et de la prestation des services (SGPS), qui en assure également le soutien.

7. Les Services de gestion des applications et services opérationnels de technologie de l'information (SGASOTI) constituent l'organe d'exécution pour les services internes de la DGSIT. Les SGASOTI exécutent des fonctions telles que l'intégration de systèmes ainsi que le développement et l'entretien des applications en vue de soutenir d'autres directions générales et régions dans la prestation de leurs programmes et de leurs services. Les SGASOTI assurent le développement d'applications Web, offrent des services de gestion des applications pour les systèmes partagés et mettent sur pied des services d'applications spécialisées. La sécurité des TI fait partie intégrante de la prestation continue des programmes et des services qu'offrent les SGASOTI.

8. Le Secteur de la gestion et de la prestation des services (SGPS) offre des services pour les ordinateurs centraux, les ordinateurs de milieu de gamme, les ordinateurs de bureau et les réseaux locaux. Le SGPS offre également des services de continuité des opérations, de reprise après sinistre, d'impression et de distribution. Tous ces services sont également soumis à la norme de GSTI.

9. La disponibilité accrue des services communs et partagés peut aider TPSGC et ses clients à satisfaire aux exigences en matière de sécurité. Bien que ces services offrent la possibilité d'accroître l'efficacité, TPSGC reconnaît que ses décisions relatives à la sécurité peuvent avoir des répercussions sur d'autres organisations.

10. L'annexe A contient un glossaire des principaux termes utilisés dans le présent rapport de vérification.

OBJECTIF DE LA VÉRIFICATION

11. L'objectif de la présente vérification était de déterminer si TPSGC s'était conformé à certaines exigences de la norme de *Gestion de la sécurité des technologies de l'information (GSTI)* pour certains systèmes de TI essentiels qui soutiennent des services essentiels

12. La vérification porte sur quatre exigences majeures de la norme de GSTI, soit:

- *La gestion des vulnérabilités* : Gérer de façon continue les menaces aux programmes, systèmes et services. Cette tâche de gestion inclut la découverte des menaces et la mise en œuvre de solutions adéquates.
- *La gestion des correctifs :* Acquérir, tester et installer des correctifs pour les logiciels d'un système de TI administré.
- *La séparation des tâches:* Répartir les responsabilités liées à une fonction du système de TI ou à une fonction de gestion de manière à éviter les situations où une seule personne peut rendre un système vulnérable à un abus non détecté.
- *Le journal de vérification de sécurité :* Enregistrer les activités liées à la sécurité, à l'intégrité et à la disponibilité d'un système.

13. Ces quatre exigences ont été sélectionnées, car elles ont été jugées par le Bureau de la vérification et de l'évaluation comme présentant un risque élevé pour le Ministère.

14. Dans le cadre de la présente vérification, certaines parties de six systèmes de TI essentiels ont été sélectionnées afin de subir les tests de vérification. Nous avons défini les systèmes de TI essentiels comme les systèmes qui étaient en place pour soutenir une fonction de gestion essentielle ou un service essentiel tel que défini dans le rapport sommaire de TPSGC portant sur l'analyse des répercussions sur les opérations, daté du 9 mars 2010. Ces six systèmes se trouvent dans la région de la capitale nationale et ont été sélectionnés parce qu'ils soutiennent de nombreux services essentiels de premier niveau devant être repris dans les 72 heures en cas de panne ou de sinistre. Les six systèmes de TI essentiels sélectionnés sont les suivants :

- Le Système de gestion de projet et des activités (SGPA) de la Direction générale des biens immobiliers;
- La solution SIGMA (le système de gestion financière et de gestion du matériel de TPSGC) de la Direction générale des finances;
- Le système de production de la Gazette du Canada de la Direction générale des conseils, de l'information et des services partagés (DGCISP);
- Le logiciel LDRPS (système évolutif de planification de la reprise du traitement après sinistre) de la Direction générale des services ministériels et des politiques stratégiques (DGSMPS);
- Le Système de gestion des documents et de l'information de l'entreprise (SGDIE) de la DGSMPS;

- Le Système d'information sur la sécurité ministérielle et industrielle (SISMI) de la DGCISP.

15. Même si la vérification était exclusivement axée sur les systèmes susmentionnés, nous prévoyons que les résultats de la présente vérification serviront à améliorer la sécurité de tous les systèmes de TI du Ministère. Par conséquent, nous nous attendons à ce que l'étendue des mesures incluses dans le Plan d'action de la gestion établi en réponse aux recommandations formulées à la suite de la vérification englobe tous les systèmes de TI essentiels et non seulement les six systèmes examinés dans le cadre la vérification.

16. La vérification n'a pas porté sur les exigences de la norme de GSTI relatives à la protection des renseignements classifiés, puisque ceux-ci sont examinés dans le cadre de la vérification de TPSGC relative aux renseignements classifiés traités électroniquement. En outre, nous n'avons pas examiné l'intégrité des données contenues dans les systèmes, et aucune demande d'accès au code des systèmes ou des applications n'a été formulée.

17. Pour obtenir plus de renseignements sur l'objectif, la portée, l'approche et les critères, voir la section « À propos de la vérification » à la fin du présent rapport.

ÉNONCÉ D'ASSURANCE

18. La présente vérification a été réalisée conformément aux *Normes internationales pour la pratique professionnelle de la vérification interne* de l'Institut des vérificateurs internes.

19. Des procédures de vérification suffisantes et appropriées ont été suivies et des éléments probants ont été recueillis pour appuyer l'exactitude des constatations et des conclusions énoncées dans le présent rapport, et fournir une assurance de niveau de vérification. Les constatations et les conclusions sont axées sur une comparaison des conditions telles qu'elles existaient alors, aux critères de vérification préétablis qui ont été acceptés par la direction. Les constatations et les conclusions s'appliquent seulement à l'entité examinée ainsi qu'à l'étendue et la période visées par la vérification.

OBSERVATIONS

ÉVALUATIONS DE LA VULNÉRABILITÉ

Les évaluations de la vulnérabilité ne sont pas toujours effectuées sur une base régulière

20. Une évaluation de la vulnérabilité est un processus qu'on utilise pour identifier les menaces potentielles pour les systèmes de TI existants. Les vulnérabilités sont des faiblesses qui pourraient permettre à une personne de s'attaquer avec succès à un système de TI. La norme de GSTI exige que les ministères évaluent sur une base régulière la vulnérabilité des systèmes très délicats ou assortis de risques importants, ainsi que la vulnérabilité des autres systèmes, sur une base facultative.

21. Les évaluations de la vulnérabilité sont importantes puisqu'elles permettent d'identifier, de quantifier et de prioriser les menaces qui pèsent sur un système de TI. En se fondant sur les informations contenues dans les évaluations de la vulnérabilité, les ministères sont en mesure de définir des solutions aux menaces identifiées.

22. Nous nous attendions à ce que TPSGC ait évalué régulièrement la vulnérabilité des systèmes TI hautement confidentiels ou hautement exposés qui sont accessibles par l'entremise de son réseau ainsi que de l'extérieur du réseau, comme l'exige la norme de GSTI. Selon le Secrétariat du Conseil du Trésor, le terme « régulièrement » signifie à intervalles fixes (par exemple, hebdomadaire, mensuel, trimestriel, etc.), en fonction de l'évaluation des risques effectuée pour le system.

23. Nous nous attendions aussi à constater, dans le cas où une évaluation de la vulnérabilité ne pouvait être réalisée au niveau de l'application, qu'une évaluation serait menée au niveau de l'infrastructure (niveau des adresses IP) des TI. Pour ce faire, il faudrait connaître toutes les adresses IP de chaque application utilisée au sein du Ministère.

24. Nous avons constaté que la vulnérabilité de l'infrastructure des systèmes de TI essentiels accessible de l'extérieur du réseau de TPSGC avait été évaluée sur une base régulière. L'évaluation de la vulnérabilité des éléments des systèmes de TI essentiels accessibles de l'intérieur de TPSGC n'étaient effectuées que si l'administrateur du système de TI essentiel en fait la demande expresse et n'étaient pas effectuées sur une base régulière. Cinq des six systèmes essentiels sélectionnés dans le cadre de la présente vérification n'étaient accessibles que par le biais du réseau interne de TPSGC.

25. Selon l'Association des professionnels de la vérification et du contrôle des systèmes d'information (ISACA), plus de 80 % de toutes les activités malveillantes sont réalisées par des employés actuels ou anciens. Le Bureau de la vérification et de l'évaluation n'a pas fait de tests concernant les activités malveillantes et n'a trouvé aucune preuve d'activités malveillantes de la part d'employés actuels ou anciens. Cependant, le risque que les

vulnérabilités puissent ne pas être détectées augmente lorsque les composantes internes des systèmes de TI essentiels ne sont pas évaluées sur une base régulière. Cette lacune pourrait donner lieu à des accès non autorisés aux systèmes de TI essentiels par l'entremise du réseau interne de TPSGC.

26. Nous avons également constaté que des évaluations de la vulnérabilité étaient effectuées au niveau de l'infrastructure des TI (au niveau de l'adresse IP). Toutefois, au moment de la vérification, la DGSIT n'a pu fournir que les adresses IP de quatre des six systèmes essentiels examinés. Par conséquent, nous n'avons pas pu déterminer si des évaluations de la vulnérabilité avaient été menées sur les deux autres systèmes essentiels. Ultérieurement à la période d'examen de la vérification, les adresses IP des six systèmes essentiels examinés ont été fournies par la DGSIT et des évaluations de la vulnérabilité n'avaient pas été menées sur les deux systèmes qui restaient.

27. Effectuer des évaluations de la vulnérabilité au niveau de l'infrastructure des TI (au niveau de l'adresse IP) donnent une certaine assurance que les vulnérabilités exposées au public sont détectées et corrigées. Toutefois, ces évaluations ne fournissent pas d'assurance pour le système dans son ensemble, puisqu'un système peut résider sur divers serveurs, et que chacun de ces serveurs possède une adresse IP différente. Par conséquent, si une seule adresse IP est testée et que les autres adresses IP ne le sont pas, le système, dans son ensemble, n'a pas été correctement évalué.

28. Des évaluations régulières et complètes de la vulnérabilité contribuent à assurer que les menaces sont identifiées en temps opportun.

Les mesures de gestion découlant des évaluations de la vulnérabilité ne font pas l'objet d'un suivi officiel

29. Une fois que les évaluations de la vulnérabilité sont effectuées, des plans d'action de la gestion sont élaborés afin de répondre aux risques et aux menaces identifiés. Le suivi des mesures de gestion pour assurer leur mise en œuvre comprend la production de rapports sur les stratégies d'atténuation utilisées pour réduire l'exposition aux faiblesses potentielles ou accepter les risques et les menaces identifiés dans les évaluations de la vulnérabilité

30. Le suivi est important, car sans celui-ci, TPSGC ne sais pas si des mesures ont été prises à l'égard des risques et des menaces identifiés, afin de réduire l'exposition aux faiblesses potentielles.

31. La norme de GSTI exige que les ministères documentent les évaluations de la vulnérabilité, les décisions ultérieures et les mesures correctives.

32. Nous nous attendions à ce que des mesures soient prises relativement aux risques et aux menaces identifiés dans les évaluations de la vulnérabilité et que la mise en œuvre des

mesures qui en résulte fasse l'objet d'un suivi officiel afin d'assurer leur pleine mise en œuvre et de diminuer l'exposition du système aux risques et aux menaces.

33. Nous avons constaté qu'il n'existait pas de procédure officielle destiné aux administrateurs de système pour faire le suivi des résultats des évaluations de la vulnérabilité. Par exemple, nous avons examiné six rapports d'évaluation comportant un total combiné de 26 vulnérabilités à haut risque. Nous avons trouvé des preuves d'activités d'atténuation pour neuf des 26 vulnérabilités relevées dans les six rapports. Les neuf vulnérabilités en question étaient incluses dans deux de ces six rapports. Les activités d'atténuation ont principalement été observées dans des courriels échangés entre l'administrateur de système et les opérations de sécurité de la DGSIT. Seules certaines de ces activités d'atténuation étaient documentées de façon officielle. Nous n'avons trouvé aucune preuve que les administrateurs de système recouraient à un processus de suivi officiel pour s'assurer que toutes les vulnérabilités à haut risque étaient corrigées. Dans le même ordre d'idées, trois vulnérabilités à haut risque et trois à moyen risque étaient identifiées dans l'évaluation de la vulnérabilité de SIGMA daté de mars 2008. Bien que le rapport de certification pour SIGMA fasse mention du rapport d'évaluation de la vulnérabilité, nous n'avons relevé aucune preuve que les vulnérabilités constatées avaient été réglées.

34. Un processus de suivi est important pour aider à s'assurer que des mesures sont prises pour contrer les menaces connues, à défaut de quoi les systèmes essentiels pourraient être vulnérables.

GESTION DES CORRECTIFS

Le processus documenté de gestion des correctifs est généralement suivi par TPSGC

35. La gestion des correctifs est une composante du processus de gestion du changement, qui consiste à acquérir, à tester et à installer des correctifs pour les logiciels sur un système de TI. Un correctif est une portion de logiciel conçue pour résoudre des problèmes de sécurité, corriger des lacunes, faciliter l'utilisation ou accroître le rendement d'un logiciel, d'un système d'exploitation ou de ses données d'appui.

36. L'objectif principal de la gestion des correctifs est de créer un environnement configuré de manière consistante, protégé contre les menaces connues visant le système d'exploitation et le logiciel d'application, et de veiller à ce que les correctifs de sécurité soient appliqués en temps opportun. Le fait de ne pas installer rapidement les correctifs de sécurité qui corrigent les nouvelles vulnérabilités peut donner lieu à des incidents de sécurité graves en matière de TI.

37. Nous nous attendions à ce que TPSGC suive la norme de GSTI en établissant un processus systématique et documenté de gestion des correctifs, et s'assure que les derniers correctifs de sécurité ont été appliqués à tous les systèmes de TI essentiels. Nous nous attendions aussi à

constater que le coordonnateur de la sécurité des TI veille à ce que ce processus soit efficace et suivi.

38. Nous avons constaté que quatre des six systèmes de TI essentiels sélectionnés étaient dotés d'un processus de gestion des correctifs approuvé permettant de s'assurer que les correctifs de sécurité sont installés en temps opportun. Ces applications suivaient le processus de gestion des correctifs du SGPS, lequel détermine les étapes ou les tâches à réaliser pour mettre en place un correctif.

39. Le cinquième système de TI essentiel sélectionné, le Système d'information sur la sécurité ministérielle et industrielle (SISMI), faisait l'objet d'un processus de gestion des correctifs, mais celui-ci n'avait pas été officiellement approuvé. Un processus de gestion des correctifs approuvé contribue à s'assurer que les correctifs sont bien gérés et mis en œuvre, et que les vulnérabilités en matière de sécurité sont corrigées.

40. Pour ce qui est du sixième système de TI essentiel, le logiciel LDRPS – Living Disaster Recovery Planning System (système évolutif de planification de la reprise du traitement après un sinistre), nous n'avons pas pu évaluer le processus de gestion des correctifs, car aucun correctif n'était disponible pour la version très personnalisée du système utilisé par TPSGC. Cette personnalisation a donné lieu à une version du logiciel LDRPS propre à TPSGC qui diffère substantiellement de la version commercialisée. Bien que des correctifs soient disponibles pour la version commerciale du logiciel LDRPS, TPSGC n'a été en mesure d'installer aucun correctif du fournisseur en raison du caractère personnalisé de sa version. En outre, la version de TPSGC du logiciel LDRPS est vieille et n'est plus soutenue par le fournisseur.

41. Étant donné qu'aucun des correctifs n'a été installé dans le logiciel LDRPS, le système du Ministère peut être exposé au risque de panne ou d'intrusion et pourrait subir une atteinte à la sécurité.

SÉPARATION DES TÂCHES

La séparation des tâches est respectée dans la plupart des cas

42. La séparation des tâches survient lorsque plus d'une personne est requise pour accomplir un travail. Elle consiste à séparer certains domaines de responsabilité ou tâches afin de réduire la fraude et les erreurs non intentionnelles.

43. La séparation des tâches est un contrôle interne de base utilisé lorsque le fait d'assigner des responsabilités conflictuelles liées à un système de TI ou à une fonction opérationnelle à une seule personne peut rendre un système vulnérable aux abus non détectés ou donner lieu à un point de défaillance unique. Par exemple, un développeur d'applications de la DGSIT ne devrait pas pouvoir approuver les résultats de ses tests finaux, car il pourrait dissimuler des

modifications non autorisées apportées à l'application. Une vérification indépendante des résultats des tests finaux fournis une assurance raisonnable que seules les modifications autorisées ont été apportées à une application.

44. Nous nous attendions à ce que les responsabilités en matière de TI soient réparties au sein de TPSGC de manière à s'assurer que le plein contrôle de tout un système de TI ou d'une fonction opérationnelle importante ne soit pas attribué à une seule personne. Les personnes autorisées à effectuer des opérations critiques ne doivent pas être chargées de vérifier ces opérations.

45. Nous avons constaté que cinq des six systèmes de TI essentiels testés faisaient l'objet d'une séparation des tâches appropriée pour prévenir des modifications non autorisées aux systèmes, aux bases de données ou aux serveurs.

46. Toutefois, nous avons constaté que quatre personnes des Services de gestion des applications et services opérationnels de technologie de l'information (SGASOTI) possédaient des droits d'« administrateur» au SISMI. Ces employés avaient un accès complet à toutes les commandes du SISMI et aux fonctions réservées du SISMI.

47. Grâce à un accès complet aux serveurs en production du SISMI, ces personnes pourraient modifier le code de programme du SISMI, modifier les bases de données du SISMI et donner ou retirer l'accès à n'importe quel utilisateur ou administrateur du système. Puisqu'il n'y avait aucun journal de vérification permettant d'identifier les utilisateurs qui avaient accédé au SISMI (voir la section portant sur les journaux de vérification de sécurité ci-dessous), des modifications non autorisées et non détectées pourraient être apportées aux données contenues dans le SISMI, y compris au code du SISMI

JOURNAUX DE VÉRIFICATION DE SÉCURITÉ

Les journaux de vérification de sécurité sont examinés pour la plupart des systèmes essentiels

48. Un journal de vérification est un registre des opérations effectuées dans un système de TI qui permet de vérifier l'activité du système. Un journal de vérification de sécurité est un sous-ensemble de journal de vérification qui porte sur les activités liées à la sécurité, à l'intégrité et à la disponibilité du système.

49. Un journal de vérification de sécurité tient un registre des activités liées à la sécurité, y compris la détermination et l'enregistrement des accès et des opérations non autorisés dans un système essentiel. Un tel journal est obligatoire pour satisfaire à la norme de GSTI.

50. Nous nous attendions à ce que tous les systèmes de TI essentiels de TPSGC soient dotés d'une fonction de journal de vérification de sécurité qui enregistre les événements pouvant

indiquer une tentative d'atteinte ou une atteinte potentielle à la sécurité ainsi que tout problème liés à l'intégrité et à la disponibilité du système.

51. Nous avons constaté que des journaux de vérification de sécurité avaient été produits et examinés dans quatre des six systèmes de TI essentiels examinés. Pour ce qui est du logiciel LDRPS, nous avons constaté la présence d'un journal de vérification de sécurité, toutefois, celui-ci n'avait pas fait l'objet d'un examen. Nous n'avons pas pu déterminer qui était responsable d'examiner les dossiers du journal de vérification de sécurité du logiciel LDRPS. Les journaux de vérification de sécurité devraient être examinés sur une base régulière.

52. La fonction de journal de vérification de sécurité est disponible dans le SISMI, mais nous avons observé qu'elle n'avait pas été activée en raison de problèmes de rendement de l'application. Toutefois, si un problème particulier devait se produire, l'enregistrement dans le journal de vérification pourrait être activé pendant une courte période.

53. L'activation ou l'examen des journaux de vérification de sécurité contribueraient à assurer que les atteintes à la sécurité du LDRPS et du SISMI soient détectées.

CONCLUSION

54. Dans l'ensemble, nous avons constaté que, pour la majorité des six systèmes de TI essentiels sélectionnés pour l'examen, TPSGC se conformait à la plupart des exigences sélectionnées de la norme de GSTI. Cependant, nous avons noté que certaines améliorations pouvaient être apportées. Nous avons observé que, pour les systèmes sélectionnés pour la présente vérification TPSGC n'avait pas toujours mené des évaluations de la vulnérabilité de manière régulière, et que les mesures correctives ne faisaient pas l'objet d'un suivi officiel.

55. Nous avons également constaté que TPSGC avait mis en place un processus systématique et documenté de gestion des correctifs afin de s'assurer que les correctifs de sécurité étaient appliqués en temps opportun. Nous avons aussi noté que, dans l'ensemble, les mécanismes de séparation des tâches étaient adéquats pour cinq des six systèmes examinés dans le cadre de la présente vérification.

56. Enfin, nous avons observé dans quatre des six systèmes sélectionnés dans le cadre de la présente vérification, que des journaux de vérification de sécurité étaient activés et faisaient l'objet d'un examen afin de détecter des atteintes potentielles.

RÉPONSE DE LA GESTION

La Direction générale des services d'infotechnologie (DGSIT) a examiné le rapport de vérification et accepte les recommandations qui y figurent. La DGSIT a élaboré un plan d'action de la gestion pour s'assurer que les recommandations de la vérification soient appliquées adéquatement.

La direction prend acte des conclusions du rapport de vérification et désire souligner que la DGSIT considère que le rapport Continuité opérationnelle et exigences essentielles en matière de TI (COEETI) 2010 de TPSGC constitue le registre définitif des systèmes essentiels du Ministère.

La direction a déjà répondu à plusieurs des recommandations incluses dans le rapport de vérification. Par exemple, la DGSIT a procédé à l'achèvement de l'évaluation de la vulnérabilité de la COEETI afin de cerner les dépendances clés entre les services critiques et les systèmes de TI. La direction a également augmenté le nombre d'évaluations de la vulnérabilité effectuées sur les interfaces externes et a amélioré les processus de surveillance des vulnérabilités découvertes au cours des évaluations et de mise en application de mesures correctives. Enfin, le Système d'information sur la sécurité ministérielle et industrielle (SISMI) a été transféré dans un centre de données géré par la DGSIT et est désormais pris en charge avec la même rigueur que les autres systèmes essentiels.

RECOMMANDATIONS ET PLAN D'ACTION DE LA GESTION

Recommandation 1 : Le Dirigeant principal de l'information, Direction générale des services d'infotechnologie, devrait mettre en place des mécanismes permettant d'assurer que tous les systèmes de TI très délicats ou assortis de risques importants qui sont soutenus par la DGSIT soient soumis de façon régulière à des évaluations de la vulnérabilité, et que les vulnérabilités identifiées fassent l'objet d'un suivi formel et soient corrigées.

> **Plan d'action de la gestion 1.1 :** Définir une norme d'évaluation de la vulnérabilité, notamment un calendrier d'examens continus de tous les systèmes de TI de niveau 1 et de tous les systèmes de TI très délicats ou assortis de risques importants de TPSGC qui sont appuyés par la DGSIT.
>
> **Plan d'action de la gestion 1.2 :** Cerner les lacunes et examiner le processus afin de satisfaire à la norme définie au point 1.1.
>
> **Plan d'action de la gestion 1.3 :** Mettre en œuvre le processus et préciser les exigences nécessaires en matière de mesures correctives afin de satisfaire à la norme d'évaluation de la vulnérabilité définie au point 1.1

Plan d'action de la gestion 1.4 : À compter de mars 2012, produire régulièrement des rapports sur la conformité pour le Coordonnateur de la sécurité de la TI. Les rapports porteront sur les activités définies pour combler les lacunes d'un statut non conforme.

Recommandation 2 : Le Dirigeant principal de l'information, Direction générale des services d'infotechnologie, devrait examiner le processus de gestion des correctifs pour tous les systèmes de TI essentiels qui sont soutenus par la DGSIT et travailler en collaboration avec les sous-ministres adjoints responsables afin d'assurer que des correctifs appropriés soient apportés aux systèmes.

Plan d'action de la gestion 2.1 : Définir une norme de gestion des correctifs, notamment un calendrier d'examens continus de tous les systèmes de TI de niveau 1 et de tous les systèmes de TI très délicats ou assortis de risques importants de TPSGC qui sont appuyés par la DGSIT.

Plan d'action de la gestion 2.2 : Cerner les lacunes en fonction de la norme définie au point 2.1.

Plan d'action de la gestion 2.3 : Déterminer les mesures correctives nécessaires pour satisfaire à la norme.

Plan d'action de la gestion 2.4 : À compter de mars 2012, produire régulièrement des rapports sur la conformité pour le Coordonnateur de la sécurité de la TI. Les rapports porteront sur les activités définies pour combler les lacunes d'un statut non conforme.

Recommandation 3 : Le Dirigeant principal de l'information, Direction générale des services d'infotechnologie, devrait examiner la séparation des tâches pour tous les systèmes de TI essentiels qui sont soutenus par la DGSIT et travailler en collaboration avec les sous-ministres adjoints responsables pour répondre aux préoccupations soulevées au sujet des responsabilités conflictuelles.

Plan d'action de la gestion 3.1 : Définir une norme de séparation des tâches, notamment un calendrier d'examens continus de tous les systèmes de TI de niveau 1 et de tous les systèmes de TI très délicats ou assortis de risques importants de TPSGC qui sont appuyés par la DGSIT.

Plan d'action de la gestion 3.2 : Cerner les lacunes en fonction de la norme définie au point 3.1.

Plan d'action de la gestion 3.3 : Déterminer les mesures correctives nécessaires pour satisfaire à la norme.

Plan d'action de la gestion 3.4 : À compter de mars 2012, produire régulièrement des rapports sur la conformité pour le Coordonnateur de la sécurité de la TI. Les rapports porteront sur les activités définies pour combler les lacunes d'un statut non conforme.

Recommandation 4 : Le Dirigeant principal de l'information, Direction générale des services d'infotechnologie, devrait examiner les fonctions de journal de vérification de sécurité de tous les systèmes de TI essentiels qui sont soutenus par la DGSIT et travailler en collaboration avec les sous-ministres adjoints responsables afin de combler les lacunes identifiées pour le logiciel LDRPS et le Système d'information sur la sécurité ministérielle et industrielle (SISMI).

Plan d'action de la gestion 4.1 : Définir une norme de surveillance des registres de contrôle de la sécurité, notamment un calendrier d'examens continus de tous les systèmes de TI de niveau 1 et de tous les systèmes de TI très délicats ou assortis de risques importants de TPSGC qui sont appuyés par la DGSIT.

Plan d'action de la gestion 4.2 : Cerner les lacunes en fonction de la norme définie au point 4.1.

Plan d'action de la gestion 4.3 : Déterminer les mesures correctives nécessaires pour satisfaire à la norme.

Plan d'action de la gestion 4.4 : À compter de mars 2012, produire régulièrement des rapports sur la conformité par rapport à la norme pour le Coordonnateur de la sécurité de la TI. Les rapports porteront sur les activités définies pour combler les lacunes d'un statut non conforme.

Recommandation 5 : Conformément aux exigences de la Politique sur la sécurité des technologies de l'information (PM 104), le Dirigeant principal de l'information, Direction générale des services d'infotechnologie, devrait fournir des conseils techniques aux sous-ministres adjoints afin d'assurer la sécurité de tous les systèmes ministériels de TI qui ne sont pas soutenus par la DGSIT, y compris des conseils pour faire en sorte que les exigences en matière d'évaluation de la vulnérabilité, de gestion des correctifs, de séparation des tâches et de journal de vérification de sécurité soient respectées.

Plan d'action de la gestion 5.1 : Fournir une orientation fonctionnelle aux SMA et aux DGR en informant le Comité ministériel sur la sécurité des responsabilités des régions et des directions générales en matière de GSTI.

Plan d'action de la gestion 5.2 : Transmettre les normes de TPSGC (précisées aux points 1.1, 2.1, 3.1 et 4.1), aux SMA et DGR concernés pour tous les systèmes de TI de niveau 1 et de tous les systèmes de TI très délicats ou assortis de risques importants de TPSGC qui ne sont pas appuyés par la DGSIT et demander qu'ils respectent ces normes.

Plan d'action de la gestion 5.3 : Demander aux SMA et aux DGR concernés de contrôler et de confirmer la conformité par rapport aux normes de TPSGC (définies aux points 1.1, 2.1, 3.1 et 4.1) et de faire rapport au Coordonnateur de la sécurité de la TI. Les rapports incluent les activités définies pour combler les lacunes d'un statut non conforme.

Plan d'action de la gestion 5.4 : À compter de mars 2012, contrôler et signaler régulièrement les plans d'action énumérés au point 5.3 au DPI.

À PROPOS DE LA VÉRIFICATION

Autorité

La présente vérification a été approuvée par le Comité de la vérification et de l'évaluation de Travaux publics et Services gouvernementaux Canada dans le cadre du Plan pluriannuel de vérification et d'évaluation axé sur les risques de 2009 à 2014.

Objectif

L'objectif de la présente vérification était de déterminer si TPSGC s'était conformé à certaines exigences de la norme de *Gestion de la sécurité des technologies de l'information (GSTI)* pour certains systèmes de TI essentiels qui soutiennent des services essentiels.

Étendue et méthode

La vérification a porté sur quatre exigences essentielles de la norme de GSTI, soit :

- *La gestion des vulnérabilités* : Gérer de façon continue les menaces aux programmes, systèmes et services. Cette tâche de gestion inclut la découverte des menaces et la mise en œuvre de solutions adéquates.
- *La gestion des correctifs :* Acquérir, tester et installer des correctifs pour les logiciels d'un système de TI administré.
- *La séparation des tâches:* Répartir les responsabilités liées à une fonction du système de TI ou à une fonction de gestion de manière à éviter les situations où une seule personne peut rendre un système vulnérable à un abus non détecté.
- *Le journal de vérification de sécurité : Enregistrer les activités liées à la sécurité, à l'intégrité et à la disponibilité d'un système.*

Ces quatre exigences ont été sélectionnées parce qu'elles ont été jugées par le Bureau de la vérification et de l'évaluation comme présentant un risque plus élevé pour le Ministère. Trois des quatre exigences sélectionnées de la norme de GSTI (gestion de la vulnérabilité, gestion des correctifs et séparation des tâches) sont incluses dans la partie II de la norme de GSTI qui porte sur l'approche ministérielle de l'organisation et de la gestion de la sécurité des TI. Cette partie de la norme contient des directives et des conseils sur la façon d'organiser et de gérer un programme de sécurité des TI. Elle porte sur les rôles et les responsabilités, les politiques, les ressources et les contrôles de gestion. La quatrième norme de GSTI sélectionnée, le journal de vérification de sécurité, est incluse dans la partie III de la norme de GSTI portant sur la détection. Ces contrôles sont utilisés pour détecter les incidents.

Dans le cadre de la présente vérification, certaines parties de six systèmes de TI essentiels ont été sélectionnées afin de subir les tests de vérification. Nous avons défini les systèmes de TI essentiels comme les systèmes qui étaient en place pour soutenir une fonction de gestion essentielle ou un service essentiel tel que défini dans le rapport sommaire de TPSGC portant sur l'analyse des répercussions sur les opérations, daté du 9 mars 2010. Ces six systèmes se trouvent dans la région de la capitale nationale et ont été sélectionnés parce qu'ils soutiennent de nombreux services essentiels de premier niveau devant être repris dans les 72 heures en cas de panne ou de sinistre. Les six systèmes de TI essentiels sélectionnés sont les suivants :

- Le Système de gestion de projet et des activités (SGPA) de la Direction générale des biens immobiliers;
- La solution SIGMA (le système de gestion financière et de gestion du matériel de TPSGC) de la Direction générale des finances;
- Le système de production de la Gazette du Canada de la Direction générale des conseils, de l'information et des services partagés (DGCISP);
- Le logiciel LDRPS (système évolutif de planification de la reprise du traitement après sinistre) de la Direction générale des services ministériels et des politiques stratégiques (DGSMPS);
- Le Système de gestion des documents et de l'information de l'entreprise (SGDIE) de la DGSMPS;
- Le Système d'information sur la sécurité ministérielle et industrielle (SISMI) de la DGCISP..

La vérification n'a pas porté sur les exigences de la norme de GSTI relatives à la protection des renseignements classifiés, puisque ceux-ci sont examinés dans le cadre de la vérification de TPSGC relative aux renseignements classifiés traités électroniquement. En outre, nous n'avons pas examiné l'intégrité des données contenues dans les systèmes, et aucune demande d'accès au code des systèmes ou des applications n'a été formulée

La présente vérification a été réalisée conformément aux *Normes internationales pour la pratique professionnelle de la vérification interne* de l'Institut des vérificateurs internes.

Au cours de la phase d'étude préparatoire, des instruments de politique ont été analysés et les membres de la Direction générale des services d'infotechnologie (DGSIT) et d'autres directions sélectionnées ont été interviewés. Une évaluation des risques a été menée et a permis de déterminer les risques liés aux éléments de la norme de GSTI. Cette évaluation des risques a pris en compte toutes les sections de la norme de GSTI, la réponse de l'auto-évaluation de la conformité de TPSGC à la norme de GSTI à la ronde VII des évaluations fondées sur le Cadre de responsabilisation de gestion (CRG) et l'évaluation initiale du SCT portant sur la conformité de TPSGC à la norme de GSTI.

Au cours de la phase d'examen, des entrevues exhaustives ont été menées auprès du personnel clé des directions générales. Les processus et les documents pertinents ont été examinés et testés. Sur la base de l'analyse de l'information et des preuves recueillies, l'équipe de vérification a formulé des observations qui ont été validées par les gestionnaires appropriés.

Critères

Les critères suivants ont été utilisés pour évaluer la conformité de TPSGC aux exigences sélectionnées de la norme de GSTI pour certaines parties de systèmes de TI essentiels de la région de la capitale nationale qui prennent en charge les services essentiels :

- TPSGC effectue régulièrement des évaluations de la vulnérabilité pour les systèmes de TI essentiels sélectionnés et les systèmes de TI accessibles de l'extérieur de TPSGC;

- TPSGC a établi un processus systématique et documenté de gestion des correctifs afin de s'assurer que les correctifs de sécurité sont appliqués en temps opportun sur les systèmes de TI essentiels sélectionnés;

- Une bonne séparation des tâches est en place pour les systèmes de TI afin d'éviter que des modifications non autorisées soient apportées aux systèmes, aux bases de données et aux serveurs;

- Les fonctions de journal de vérification de sécurité font partie des systèmes de TI essentiels sélectionnés et sont activées.

Fin des travaux de vérification

Les travaux sur le terrain menés dans le cadre de la présente vérification ont été pour l'essentiel terminés le 1er août 2010.

Équipe de vérification

La vérification a été menée par le personnel du Bureau de la vérification et de l'évaluation et un vérificateur consultant, supervisé par le Directeur de la Vérification interne et sous la direction générale de la Dirigeante principale de la vérification et de l'évaluation.

La vérification a été examinée par la fonction d'examen de la qualité du Bureau de la vérification et de l'évaluation.

Annexe A

Glossaire

Systèmes de TI essentiels	Des systèmes qui sont en place pour soutenir une fonction de gestion essentielle ou un service essentiel. La DGSIT juge un système essentiel à une direction générale cliente s'il est doté d'un plan de reprise après sinistre financé.
Services essentiels	Un service dont la compromission en matière de disponibilité ou d'intégrité résulterait en un degré élevé de préjudice pour la santé, la sécurité ou le bien-être économique de la population canadienne ou pour le fonctionnement efficace du gouvernement du Canada, et qui doit être récupéré dans les premières 72 heures (classé comme niveau un) dans le rapport de TPSGC portant sur l'analyse des répercussions sur les opérations.
Adresse IP	Un code numérique qui identifie tous les périphériques qui sont connectés à un réseau ou à Internet.
Régulièrement	Un calendrier établi (hebdomadaire, mensuel, trimestriel, etc.) fondé sur une évaluation des risques effectuée sur le système. Une activité périodique et planifiée qui est conforme à la tolérance au risque du Ministère.
Gestion des correctifs	1) Un domaine de gestion des systèmes qui consiste à acquérir, mettre à l'essai et installer plusieurs correctifs (modifications au code) sur un système informatique administré. 2) Un processus qui consiste à utiliser une stratégie et un plan établissant sur quels systèmes quels correctifs doivent être appliqués et à quel moment les appliquer.
Système de TI	Les systèmes de TI sont composés non seulement d'une infrastructure, mais aussi de logiciels. Un système de TI est constitué d'un ensemble d'équipements et de programmes informatiques utilisés ensemble dans un but précis.