Rapport final

2006-714

Vérification des processus de certification et d'accréditation visant à atténuer les risques en matière de sécurité pour les applications opérationnelles de TPSGC

Bureau de la vérification et de l’évaluation

Le 28 janvier 2010

Travaux publics et Services gouvernementaux Canada
Public Works and Government Services Canada
Canada

TABLE DES MATIÈRES

POINTS SAILLANTS

Objet

i. Le but de la certification est de vérifier que les exigences en matière de sécurité établies par l'accréditeur pour un système de technologie de l'information (TI) particulier sont respectées, et que les contrôles et les mesures de protection fonctionnent comme prévu. L'autorité de certification examine et évalue les éléments probants ou les livrables de certification fournis par l'accréditeur dans le cadre du processus de certification et d'accréditation (C et A). Les exigences d'éléments probants diffèrent selon le niveau de risque auquel le système de TI est assujetti. Ces éléments probants peuvent comprendre le résultat de tout énoncé applicable relatif à la nature délicate de l'information; de l'évaluation de la menace et des risques (EMR); de l'analyse des incidences sur les activités; de l'évaluation des répercussions sur la protection des renseignements personnels; de l'estimation de la vulnérabilité; des tests de sécurité, en plus de l'information sur les produits; des autoévaluations; des vérifications et des examens de la sécurité; des évaluations stratégiques ou juridiques, etc. Le but de l'accréditation est de signifier que la direction a autorisé l'exploitation du système et qu'elle a accepté le risque résiduel qui en découle. Cette décision est fondée sur la recommandation formulée par l'autorité de certification et sur d'autres considérations de gestion comme la nécessité ou l'obligation d'offrir un service avant une date précise.

ii. Au sein de Travaux publics et Services gouvernementaux Canada (TPSGC), les responsables des directions générales (c.-à-d. les sous-ministres adjoints et les présidents-directeurs généraux) agissent comme accréditeurs de leurs applications opérationnelles ministérielles respectives, et le directeur de la sécurité de la TI du Bureau du dirigeant principal de l'information est l'autorité de certification pour ces applications opérationnelles ministérielles ainsi que pour les applications opérationnelles communes. Pour ces dernières, comme pour l'infrastructure de TI commune, l'accréditeur est le dirigeant principal de l'information du gouvernement du Canada. Un directeur du Secteur du dirigeant principal de la technologie agit comme autorité de certification pour l'infrastructure de TI commune.

iii. Lorsque les exigences de sécurité relatives aux applications opérationnelles ont été respectées et que le risque lié à l'exploitation de l'application opérationnelle a été vérifié par l'autorité de certification et jugé acceptable par l'accréditeur, l'application opérationnelle est considérée comme dûment certifiée et accréditée. Sinon, l'accréditeur peut accorder une autorisation d'exploitation provisoire. Il s'agit d'une autorisation écrite provisoire permettant, en raison de circonstances atténuantes, d'effectuer le traitement d'information sensible (voir l'annexe A pour la définition) lorsque le risque résiduel n'est pas encore jugé acceptable, mais qu'il existe un besoin opérationnel d'utiliser l'application. Les conditions liées à une autorisation d'exploitation provisoire peuvent nécessiter la mise en place de mesures de protection temporaires pendant que la conception, le développement et l'essai de l'application

opérationnelle sont en cours. Une autorisation d'exploitation provisoire comporte diverses conditions comme le type d'information qui peut être traité et la date d'expiration.

iv. La vérification a porté sur les processus de certification et d'accréditation de TPSGC mis en place pour les applications opérationnelles existantes qui ont été recensées dans le cadre du projet de conformité à la gestion de la sécurité des technologies de l'information ainsi que pour les nouvelles applications opérationnelles ayant été certifiées et accréditées depuis avril 2007.

Pertinence

v. La *norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI)* de 2004, qui complète la *Politique sur la sécurité* du *gouvernement*, confère aux ministères le mandat de faire certifier et accréditer les systèmes existants, y compris les applications opérationnelles, ainsi que les nouveaux systèmes avant que leur exploitation soit autorisée. Sans une certification et accréditation appropriée, un système fonctionne ou entre en exploitation sans respecter les normes du gouvernement du Canada, ce qui accroît le risque de défaillance du système, de perte de données essentielles et de problèmes relatifs à l'intégrité des données.

vi. Outre la conformité à la politique, une étape clé de la réduction des risques associés à un système consiste à mettre en place des processus de certification et d'accréditation afin de s'assurer que l'accréditeur, qui accepte en dernier ressort les risques liés à l'exploitation des applications opérationnelles, connaît la nature de ces risques et prend les mesures nécessaires pour les réduire à un niveau acceptable.

Constatations

vii. Les rôles, les responsabilités et la responsabilisation relatifs à la certification et à l'accréditation des applications opérationnelles et de l'infrastructure de TI sont définies dans un ensemble hiérarchisé de politiques et de normes émises par le Secrétariat du Conseil du Trésor du Canada et TPSGC. En date d'août 2009, le Ministère comptait environ 319 applications opérationnelles existantes, auxquelles correspond un niveau de risque élevé, moyen ou faible. La majorité de ces applications sont actuellement exploitée conformément à une autorisation d'exploitation provisoire. Il s'agit d'une pratique acceptable qui donne aux responsables des directions générales de TPSGC, en tant qu'accréditeurs de leurs applications opérationnelles respectives, le temps nécessaire pour remplir les conditions particulières afin que ces applications soient dûment certifiées et accréditées. En signant ces autorisations d'exploitation provisoires, les responsables des directions générales de TPSGC acceptent les risques associés à l'exploitation des applications opérationnelles et sont informés de l'état d'avancement du processus complet de certification et d'accréditation. Le Ministère a mis en place un processus

de reconnaissance et de suivi des applications opérationnelles existantes, ce qui permet de s'assurer que toutes les applications opérationnelles sont gérées de manière appropriée.

viii. En octobre 2008, la Direction générale des services d'infotechnologie a entrepris un projet visant à suivre la présentation des éléments probants nécessaires pour obtenir la certification et l'accréditation complète des applications opérationnelles en place. En août 2009, le processus de certification et d'accréditation était terminé pour 53 applications opérationnelles (15 sur 30 ayant un niveau de risque élevé; 9 sur 134, un niveau de risque moyen; 29 sur 155, un niveau de risque faible). Les éléments probants ont été fournis pour 14 des 15 applications opérationnelles à risque élevé restantes et ces applications sont en attente de certification et d'accréditation. Toutefois, pour un nombre important d'applications opérationnelles à risque moyen (64 sur 134) et à risque faible (82 sur 155), il reste encore à fournir les éléments probants à la Direction générale des services d'infotechnologie en vue d'obtenir la certification. Finalement, même si la norme de GSTI exige une évaluation de la menace et des risques pour chaque application opérationnelle, TPSGC ne l'exige pas pour les applications opérationnelles existantes qui ont un niveau de risque faible.

ix. Bien que le Ministère ait mis en place un processus clair pour l'obtention de la certification et de l'accréditation complète de ses applications opérationnelles existantes, ce processus ne s'applique pas aux nouvelles applications opérationnelles. Même s'il existe trois documents d'orientation concernant la certification et l'accréditation des nouvelles applications opérationnelles, ces documents n'exigent pas les mêmes produits livrables, et seul l'un d'entre eux a été officiellement approuvé par la Direction générale des services d'infotechnologie. De plus, les accréditeurs n'ont pas accepté ces documents d'orientation. La certification et l'accréditation des nouvelles applications opérationnelles constituent un processus continu. Depuis avril 2007, dix-sept nouvelles applications opérationnelles ont été certifiées et accréditées. Le processus d'évaluation de la qualité en place donne à la direction l'assurance que le processus de certification et d'accréditation est bien exécuté.

Réponse de la gestion

La Direction générale des services d'infotechnologie est en accord avec les deux recommandations du plan d'action de gestion et nous avons préparé des mesures pour les aborder en conséquence.

Recommandations et plan d'action de la gestion

Recommandation 1 : Le président-directeur général de la Direction générale des services d'infotechnologie devrait s'assurer que le processus de certification et d'accréditation des applications opérationnelles existantes de niveau de risque faible

exige une évaluation de la menace et des risques, et que les exigences de cette évaluation reflètent le risque associé à l'application opérationnelle.

> **Plan d'action de gestion 1.1 :** Conformément à la politique sur la Gestion de la sécurité des technologies de l'information du Secrétariat du Conseil du Trésor, toutes les directions générales ont été soumises à un processus rigoureux qui visait à déterminer le degré d'exposition aux risques de leurs applications opérationnelles surannées. Les résultats de ce processus ont été répartis en trois catégories (risque faible, risque moyen et risque élevé) et enregistrés dans la fiche de sécurité pour les secteurs d'affaires. Les directions générales ont également présenté un énoncé de nature délicate pour chacune de leurs applications opérationnelles surannées à faible risque. De plus, la Direction de la sécurité de la TI, qui est l'autorité ministérielle responsable de la certification et de l'accréditation, a validé les résultats de l'énoncé de nature délicate afin de garantir qu'aucune autre tâche de gestion des risques liés à la sécurité ne soit nécessaire. La Direction générale des services d'infotechnologie consultera le Secrétariat du Conseil du Trésor afin de s'assurer que les processus liés à la fiche de sécurité pour les secteurs d'affaires, à l'énoncé de nature délicate ainsi que la validation de la certification de la Direction de la sécurité de la TI sont conformes à l'article 12.3.2 de la norme opérationnelle de gestion de la sécurité des technologies de l'information en ce qui a trait à l'évaluation des menaces et des risques des applications opérationnelles surannées à risque faible, avant le 30 avril 2010.
>
> **Plan d'action de gestion 1.2:** Si le Conseil du Trésor du Canada rejette le point 1, les directions générales devront effectuer une évaluation de la menace et des risque pour leurs applications opérationnelles surannées à faible risque avant le 31 mars 2010.

Recommandation 2 : Le président-directeur général de la Direction générale des services d'infotechnologie devrait clarifier qu'il existe un processus de certification et d'accréditation commun pour toutes les nouvelles applications opérationnelles de TPSGC, qui serait tout à fait conforme aux instruments de politique obligatoires applicables du gouvernement du Canada. Ce processus devrait être accepté par les responsables des directions générales de TPSGC, approuvé par le président-directeur général de la Direction générale des services d'infotechnologie et communiqué aux directions générales de TPSGC.

Plan d'action de gestion 2.1 : À TPSGC, l'Office du dirigeant principal de l'information détient l'autorité ministérielle sur le processus de la certification et l'accréditation. Le document intitulé « Cadre de travail sur la sécurité des applications » daté septembre 2008 est le processus utilisé par la Direction générale des services d'infotechnologie pour les nouveaux développements. Il sera présenté au comité directeur de la gestion de l'information et technologie de l'information pour acceptation comme norme ministérielle avant le 31 mars 2010.

INTRODUCTION

1. La *Politique sur la sécurité du gouvernement de 2002* comporte des exigences pour la protection des biens du gouvernement, y compris l'information. Selon l'une de ces exigences, les ministères doivent certifier et accréditer les systèmes de technologie de l'information avant leur exploitation. Dans la politique de 2002, « certification » est défini comme l'« évaluation complète des dispositifs de sécurité techniques et non techniques d'un système des TI et d'autres mesures de sauvegarde connexes, effectuée à l'appui de l'accréditation, pour déterminer le degré selon lequel un modèle de conception et de mise en œuvre précis satisfait à un ensemble donné d'exigences en matière de sécurité » et « accréditation » comme l'« autorisation officielle par la direction d'exploiter un système des TI et l'acceptation par la direction du risque résiduel s'y rattachant. L'accréditation dépend des résultats de la certification ainsi que d'autres considérations de gestion. » La *Politique sur la sécurité du gouvernement de 2002* n'indique pas ce que constitue un processus de certification et d'accréditation approuvé.

2. La *Politique sur la sécurité du gouvernement* est complétée par les diverses normes de sécurité opérationnelle du Secrétariat du Conseil du Trésor. L'une de ces normes est la *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI)* de 2004. La norme de GSTI définit les exigences sécuritaires de base que les ministères fédéraux doivent satisfaire pour assurer la sécurité de l'information et des biens de technologie de l'information (TI) placés sous leur contrôle. Selon cette norme, l'évaluation de la menace et des risques permet d'établir les exigences en matière de sécurité, les ministères doivent appliquer des mesures de sécurité supérieures aux exigences de base lorsqu'une évaluation de la menace et des risques le justifie, et une telle évaluation doit être menée pour chaque système.

3. Voici les étapes clés d'une évaluation de la menace et des risques, telles qu'elles sont établies dans la norme de GSTI :
   - identifier et classer l'information et les biens connexes selon leur degré de délicatesse (Voir l'annexe A pour la définition) (et consigner cette information dans un énoncé de la nature délicate);
   - évaluer les vulnérabilités du système et les menaces à son endroit qui pourraient avoir une incidence sur la prestation d'un programme ou d'un service;
   - déterminer le niveau de risque, en fonction des mesures de protection en place et des vulnérabilités du système;
   - recommander des mesures de protection qui permettront de ramener le risque à un niveau acceptable.

4. L'une des exigences contenues dans la norme de GSTI concerne la certification et l'accréditation. Cette exigence oblige les ministères à faire certifier et accréditer leurs systèmes existants ainsi que les nouveaux systèmes avant que leur exploitation soit autorisée. La quantité et la qualité des éléments probants en vue de la certification

exigés par l'accréditeur dépendent de divers facteurs, comme la nature délicate de l'information qui sera traitée et la criticité du système. Ces éléments probants peuvent inclure les résultats de tout énoncé de la nature délicate applicable, de l'évaluation de la menace et des risques, de l'évaluation des incidences sur les activités, de l'évaluation des répercussions sur la protection des renseignements personnels, de l'estimation de la vulnérabilité, des tests de sécurité, en plus de l'information sur les produits, des autoévaluations, des vérifications et des examens de sécurité, et des évaluations juridiques et stratégiques qui établissent la conformité aux lois et aux politiques pertinentes.

5. L'accréditeur est responsable des applications opérationnelles sous son contrôle, qu'il exploite ou non l'infrastructure de TI autour de laquelle s'articulent les applications opérationnelles. À TPSGC, les responsables des directions générales (c.-à-d. les sous-ministres adjoints et les présidents-directeurs généraux) agissent à titre d'accréditeurs de leurs applications opérationnelles ministérielles respectives. Pour les applications opérationnelles communes et l'infrastructure de TI commune (tels les services partagés de technologie de l'information), l'accréditeur est le dirigeant principal de l'information du gouvernement du Canada. Les services partagés de technologie de l'information font partie de la Direction générale des services d'infotechnologie qui offre des services partagés à tous les ministères fédéraux, y compris TPSGC. Il incombe à l'accréditeur d'accepter les risques associés à l'exploitation d'une application opérationnelle. Il se charge aussi de la mise en œuvre des mesures de protection visant à réduire le risque à un niveau acceptable. Les risques qui demeurent une fois que le processus de certification et d'accréditation est terminé sont appelés « risques résiduels ».

6. Pour accréditer une application opérationnelle, l'accréditeur se fie aux recommandations de l'autorité de certification et à d'autres considérations de gestion telles que la nécessité ou l'obligation d'offrir un service à une certaine date. L'autorité de certification est chargée de fournir des indications sur le niveau d'effort nécessaire pour produire la documentation de certification requise et de préparer un rapport de certification et une lettre d'accréditation à l'intention de l'accréditeur. Ces documents indiquent le risque résiduel et comprennent une recommandation relativement à l'acceptation ou au rejet de ce risque résiduel. Dans certains cas, l'autorité de certification peut recommander que soit accordée une autorisation d'exploitation provisoire par l'accréditeur pendant une certaine période, avant que le processus de certification et d'accréditation soit terminé. Cette autorisation provisoire est assortie de conditions spécifiées par l'autorité de certification.

7. Depuis mai 2006, TPSGC compte deux autorités de certification. Le directeur de la Direction de la sécurité de la TI, du Bureau du dirigeant principal de l'information, est chargé de la certification de toutes les applications opérationnelles du Ministère. Il agit également comme autorité de certification pour les applications opérationnelles communes. De plus, un directeur du Secteur du dirigeant principal de la technologie

s'occupe de la certification de l'infrastructure de TI commune prise en charge par les services partagés de technologie de l'information.

8. Lors de l'adoption de la norme de GSTI, qui est obligatoire en raison de sa nature, il était prévu que la conformité du Ministère soit assurée d'ici décembre 2006. En réponse aux exigences du Secrétariat du Conseil du Trésor relatives à la norme de GSTI, TPSGC a mis sur pied un projet de conformité à cette norme. Ce projet s'est déroulé de juin 2005 à mars 2008. Outre la conformité à la GSTI pour l'ensemble du Ministère, le projet a porté sur les exigences de certification et d'accréditation contenues dans la norme.

9. Avant que se termine cette vérification, la *Politique sur la sécurité* 2002 a été remplacée en juillet 2009 par la *Politique sur la sécurité du gouvernement*. Cette nouvelle politique ne fait pas référence à la nécessité d'obtenir une certification et une accréditation. Toutefois, la norme de GSTI de 2004, qui en fait mention, est toujours en vigueur. En conséquence, il n'y a pas d'impacte matériel sur cette vérification en raison du remplacement de la politique de 2002 par la politique de 2009.

OBJECTIF DE LA VÉRIFICATION

10. La vérification a porté sur le processus de certification et d'accréditation en place à TPSGC pour les applications opérationnelles du Ministère, existantes ou nouvelles, en vue d'aider à s'assurer que les menaces et les risques de sécurité relevés pour les applications opérationnelles de TPSGC sont atténués à l'aide de mesures appropriées ou qu'ils soient acceptés par le niveau de direction approprié avant que l'utilisation des applications ne soit autorisée. Plus spécifiquement notre vérification se concentre sur les activités et l'orientation en matière de certification et d'accréditation relatives à ces applications opérationnelles, et les rapports sur les objectifs de certification et d'accréditation des applications opérationnelles, compris dans l'initiative de conformité de la GSTI de TPSGC.

11. Notre vérification n'a pas été conçue pour évaluer les risques en matière de sécurité liés à ces applications ou à la gestion continue de ces risques.

12. L'objectif de vérification inclus les opérations de TPSGC et de nouvelles applications de gestion. La vérification ne portait pas sur les processus de certification et d'accréditation pour l'infrastructure des services partagés de technologie de l'information, dont TPSGC assume la gestion en tant que fournisseur de services partagés de technologie de l'information aux ministères, y compris à TPSGC.

13. De plus amples renseignements sur l'objectif, la portée, l'approche et les critères de cette vérification figurent à la fin de ce rapport, dans la section intitulée « À propos de la vérification ».

ÉNONCÉ D'ASSURANCE

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

15. 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

Les rôles, les responsabilités et la responsabilisation relatifs à la certification et à l'accréditation sont définis

16. Les rôles et les responsabilités définissent ce dont le titulaire d'un poste donné est responsable et justiciable. Il est important que les rôles et les responsabilités relatifs à la certification et à l'accréditation soient définis, attribués et respectés pour aider à assurer la sécurité de l'information confiée à TPSGC. Nous nous attendions à ce que les rôles et les responsabilités relatifs à la sécurité des applications opérationnelles soient définis, attribués et respectés.

17. Nous avons constaté que les rôles et les responsabilités relatifs à la certification et à l'accréditation des applications opérationnelles sont définis et assignés, et qu'il n'existe aucun cas où les rôles ne sont pas respectés. Plus particulièrement, la gestion de la sécurité de la TI pour les applications opérationnelles est définie dans un ensemble hiérarchisé de politiques et de normes émises par le Secrétariat du Conseil du Trésor du Canada et TPSGC. La norme de GSTI confie aux gestionnaires de la prestation des services et des programmes la responsabilité de déterminer les exigences de sécurité de la TI des systèmes dont ils ont le contrôle, y compris les applications opérationnelles, de les faire accréditer et d'accepter le risque résiduel qui y est associé. À TPSGC, les responsables des directions générales se sont vu attribuer le rôle de gestionnaires de la prestation des services et des programmes et celui d'accréditeurs pour les applications opérationnelles dont ils ont la charge. La politique ministérielle de 2003 sur le *Programme de sécurité de la technologie de l'information* (PM-055) définit les rôles et les responsabilités en matière de sécurité de la TI à TPSGC et attribue la fonction de certification des applications opérationnelles au directeur de la Direction de la sécurité de la TI. L'autorité de certification et les accréditeurs de TPSGC se conforment à leurs rôles en recommandant et en accréditant respectivement les applications opérationnelles.

18. Les postes clés indiqués dans la PM-055 ne correspondent pas à l'organisation actuelle du Ministère ni aux postes indiqués dans le rapport d'état de la conformité à la norme de GSTI présenté en décembre 2006 au Secrétariat du Conseil du Trésor du Canada. Par exemple, la PM-055 ne reflète pas le fait que TPSGC compte deux autorités de certification. De plus, elle n'indique pas qui remplit la fonction d'accréditeur pour les applications opérationnelles ministérielles et communes. Bien qu'il n'y ait pas un sérieux manque dans la définition de la fonction, cette omission peut prêter à confusion de la part des gestionnaires de TPSGC responsables de la mise en œuvre du Programme de sécurité de la TI dans leur unité organisationnelle.

Les risques associés aux applications opérationnelles existantes ont été acceptés, et les accréditeurs sont informés de l'état d'avancement du processus de certification et d'accréditation pour ces applications

19. Les applications opérationnelles de TPSGC sont exposées à des risques divers. Un risque peut se définir comme « l'incertitude qui entoure des événements et des résultats futurs ». Nous nous attendions à ce que, à titre d'accréditeurs de leurs applications opérationnelles, les responsables des directions générales aient reconnu et accepté les risques associés à l'exploitation d'applications opérationnelles. Nous nous attendions également à ce que des rapports pertinents soient préparés à l'intention des accréditeurs sur les progrès concernant la certification et l'accréditation des applications opérationnelles existantes. Il s'agit d'un élément important puisque les accréditeurs ont la responsabilité de leurs applications opérationnelles.

20. Nous avons constaté que le Bureau du dirigeant principal de l'information a demandé aux accréditeurs d'examiner et d'accepter officiellement les autorisations d'exploitation provisoires pour leurs applications opérationnelles existantes, en décembre 2006. Ces autorisations provisoires comportent quatre conditions relatives à la certification et à l'accréditation en vue de l'acceptation. Ces conditions sont les suivantes :

- L'élaboration d'un plan d'atténuation des risques en matière de TI, en consultation avec le dirigeant principal de l'information ou son représentant, pour toutes les applications opérationnelles évaluées à risque élevé afin de réduire le risque associé à un niveau acceptable sur le plan opérationnel;
- La confirmation de l'affectation d'un agent de sécurité de la TI de la direction générale à chaque application ou groupe d'applications. La liste des agents devait être fournie pour le 31 mars 2007;
- L'assurance que les systèmes utilisés et les serveurs exploités selon le domaine de compétence des directions générales font l'objet d'un contrôle officiel de la configuration, et que les retouches essentielles aux systèmes sont déployées rapidement. La procédure appropriée devait être mise en place pour le 31 mars 2007;

- L'élaboration d'un énoncé de la nature délicate pour chaque application ou groupe d'applications.

21. La quatrième condition était la plus importante puisqu'elle nécessitait l'élaboration d'un énoncé de la nature délicate pour chaque application ou groupe d'applications conformément à l'échéancier suivant :

    - l'énoncé pour les applications à risque élevé devait être terminé pour le 31 mars 2007;
    - l'énoncé pour les applications à risque moyen devait être terminé pour le 30 juin 2007;
    - l'énoncé pour les applications à risque faible devait être terminé pour le 30 novembre 2007.

22. En août 2009, le calendrier n'avait pas été respecté, et les éléments probants, incluant des énoncés de la nature délicate, en vue de la certification d'un grand nombre d'applications opérationnelles existantes à risque moyen (64 sur 134) et à risque faible (82 sur 155) n'avaient pas encore été fournis à la Direction générale des services d'infotechnologie.

23. En 2007, en l'absence de certification et d'accréditation des applications opérationnelles existantes, les accréditeurs ont dû signer de nouvelles autorisations d'exploitation provisoires puisque les autorisations provisoires de décembre 2006 prenaient fin. Cette pratique de renouvellement des autorisations d'exploitation provisoires se poursuit en date d'avril 2009. En signant les autorisations d'exploitation provisoires, les accréditeurs acceptaient et reconnaissaient les risques associés à l'exploitation des applications opérationnelles qui soutenaient les activités de leur direction générale. Ils étaient également informés de l'état d'avancement du processus de certification et d'accréditation.

Des progrès ont été réalisés dans l'inventaire des applications opérationnelles existantes

24. Les applications opérationnelles existantes sont des applications utilisées pour soutenir les activités du ministère, dont l'exploitation a commencé avant le projet de conformité à la GSTI. Il est important de dresser un inventaire des applications opérationnelles existantes afin d'assurer leur gestion appropriée. Nous nous attendions à ce que les applications opérationnelles existantes aient été relevées.

25. Nous avons constaté que des progrès ont été réalisés dans le cadre du projet de conformité à la GSTI de TPSGC relativement à l'établissement de l'inventaire des applications opérationnelles existantes dans le Ministère, et à leur classification en fonction du risque qui leur est associé. Le processus d'inventaire des applications opérationnelles nécessite que les accréditeurs confirment la liste de leurs applications opérationnelles existantes dans le cadre du renouvellement des autorisations

d'exploitation provisoires. Nous n'avons toutefois pas effectué de tests pour nous assurer que toutes les applications opérationnelles existantes ont été inventoriées.

26. Le nombre d'applications opérationnelles existantes varie dans le temps, puisque certaines sont mises hors service. En mars 2008, 36 applications opérationnelles ont été considérées à risque élevé; 190, à risque moyen; 204, à risque faible. En août 2009, le nombre des applications opérationnelles existantes avait diminué, et il y avait alors 30 applications opérationnelles à risque élevé, 134, à risque moyen et 155, à risque faible. Cette diminution montre que le Ministère a mis en place un processus d'inventaire et de suivi de ses applications opérationnelles existantes, ce qui lui permet de s'assurer que la gestion de toutes les applications opérationnelles est appropriée.

Progrès lent dans la certification et l'accréditation des applications opérationnelles existantes

27. Il est important que les applications opérationnelles soient certifiées et accréditées en temps opportun afin d'assurer que les risques auxquels elles sont exposées soient connus et acceptés. Nous nous attendions à un seul processus documenté de certification et d'accréditation que les accréditeurs pourraient suivre. Nous nous attendions également à ce que les accréditeurs produisent, selon les échéanciers établis dans les autorisations d'exploitation provisoires, tous les livrables de certification exigés.

28. Nous avons constaté qu'il existe un seul processus de certification et d'accréditation et que les accréditeurs le suivent de manière constante pour les applications opérationnelles ayant obtenu une certification et une accréditation complètes. Nous avons également constaté qu'à compter de mars 2008, date d'achèvement du projet de conformité de la Gestion de la sécurité des technologies de l'information (GSTI), aucune application opérationnelle existante n'a obtenu une certification et une accréditation complètes. En outre, le rapport de mars 2008 sur l'avancement des travaux relatifs à la certification et à l'accréditation de la GSTI des Services de gestion des applications et services opérationnels de TI (SGASOTI) indique que l'autorité de certification avait reçu les livrables de certification uniquement pour:

- 25 des 36 applications opérationnelles évaluées à risque élevé;
- 50 des 190 applications opérationnelles évaluées à risque moyen;
- 36 des 204 applications opérationnelles évaluées à faible risque.

29. Après l'achèvement du projet de conformité de la GSTI de TPSGC en mars 2008, un nouveau projet a été lancé. Le projet de conformité des preuves de la sécurité des applications (CPSA) avait pour objectif de traiter les applications opérationnelles de TPSGC en attente, pour lesquelles les livrables de certification n'avaient pas encore été livrés à l'autorité de certification. Le résumé de projet d'août 2009 indique ce qui suit :

- des preuves ont été présentées pour 29 des 30 applications opérationnelles à risque élevé, parmi lesquelles 15 ont été certifiées et accréditées;
- des preuves ont été présentées pour 70 des 134 applications opérationnelles à risque moyen, parmi lesquelles 9 ont été certifiées et accréditées;
- des preuves ont été présentées pour 73 des 155 applications opérationnelles à faible risque, parmi lesquelles 29 ont été certifiées et accréditées.

30. Les livrables de base de certification, comme les énoncés de la nature délicate et les évaluations de la menace et des risques (EMR) n'ont pas encore été présentés à l'autorité de certification pour un certain nombre d'applications opérationnelles existantes à risque moyen et à faible risque. Par conséquent, il est possible que certains risques pour les applications opérationnelles existantes n'aient pas été reconnus.

Les directions générales ne sont pas tenues de produire des évaluations de la menace et des risques pour les applications opérationnelles existantes à faible risque

31. La norme de GSTI du gouvernement du Canada exige que les ministères réalisent des EMR pour toutes les applications opérationnelles. Les EMR aident à déterminer les risques liés à la sécurité. Ces évaluations peuvent être courtes et simples, ou beaucoup plus détaillées et rigoureuses, selon le niveau de sensibilité, de criticité et de complexité des applications opérationnelles qui en font l'objet. Nous nous attendions à ce que le processus de certification et d'accréditation pour les applications opérationnelles existantes exige la réalisation d'EMR pour toutes les applications opérationnelles ministérielles, conformément à la norme de GSTI.

32. Dans le cadre du projet de conformité de la GSTI du Ministère et du projet de CPSA subséquent, des échéances ont été établies pour la réalisation des EMR pour toutes les applications opérationnelles existantes à risque élevé et moyen. Les applications opérationnelles à faible risque ne sont pas visées par cette exigence.

33. La valeur de la réalisation d'EMR pour les applications opérationnelles à faible risque réside dans le fait qu'elles aident à déterminer les risques qui doivent être atténués de façon formelle et structurée. Elles aident également à confirmer qu'il s'agit bien d'une application opérationnelle à faible risque. De plus, en l'absence de l'exigence d'une EMR, le processus de certification et d'accréditation suivi pour certifier et accréditer les applications opérationnelles existantes à faible risque n'est pas pleinement conforme à la norme de GSTI. Bien que la conformité du processus de certification et d'accréditation pour les applications opérationnelles à faible risque soit importante, il est également important que l'exigence précise et le niveau de détail et d'analyse dont il doit être tenu compte dans les EMR reflètent le risque lié à l'application opérationnelle.

TPSGC ne dispose pas d'un processus clair pour obtenir la certification et l'accréditation des nouvelles applications opérationnelles

34. Les documents d'orientation sur la certification et l'accréditation fournissent les renseignements nécessaires à tous ceux qui participent au processus de certification et d'accréditation. Il est important de disposer de documents d'orientation clairs qui permettent aux accréditeurs de déterminer les livrables de certification qui doivent être fournis en vue de l'obtention de la certification et de l'accréditation de leurs applications opérationnelles. Il importe également que les accréditeurs suivent l'orientation fournie afin que les nouvelles applications opérationnelles soient certifiées et accréditées de façon cohérente. Nous nous attendions à un seul processus documenté de certification et d'accréditation que les accréditeurs pourraient suivre.

35. Nous avons constaté que trois documents d'orientation offrent un processus de certification et d'accréditation des nouvelles applications opérationnelles. En mai 2000, la Direction de la sécurité de la technologie de l'information a produit le « Cadre de gestion des risques pour la sécurité des TI ». Le Secteur des SGASOTI au sein de la Direction générale des services d'infotechnologie a élaboré un document intitulé « Introduction au Cadre de gestion de la sécurité des applications », daté de septembre 2008, qui décrit le processus de certification et d'accréditation pour les systèmes de TI développés, maintenus ou soutenus par les SGASOTI. En outre, la Direction générale des services d'infotechnologie (DGSIT) a élaboré une ébauche d'un document intitulé « Guide de gestion des projets de la DGSIT – volume un », daté d'avril 2008, qui décrit, entre autres, un processus pour l'obtention de la certification et de l'accréditation.

36. L'orientation concernant la liste des livrables à fournir pour l'obtention de la certification et de l'accréditation des nouvelles applications opérationnelles contenue dans ces documents n'est pas cohérente. Par exemple, les exigences à l'égard de la production d'énoncés de la nature délicate, d'EMR, d'analyses des répercussions sur les activités, d'évaluations des facteurs relatifs à la vie privée, du concept des opérations, de l'architecture et des documents relatifs aux essais, etc., sont différentes dans les trois documents. Par exemple, le « Guide de gestion des projets de la DGSIT – volume un » n'exige pas la production d'un énoncé formel de la nature délicate ou d'un EMR pour les projets de moyenne et de petite envergure.

37. Les accréditeurs peuvent être perplexes quant au processus de certification et d'accréditation à suivre et aux livrables de certification à fournir pour obtenir la certification et l'accréditation de leurs applications opérationnelles. Cette confusion peut mener à des efforts et à des dépenses inutiles de la part des accréditeurs dans le cadre de l'élaboration des livrables de certification et à des retards dans l'obtention de l'accréditation sans condition associée.

Les processus documentés de certification et d'accréditation pour les nouvelles applications opérationnelles n'ont pas été acceptés par les accréditeurs

38. Un processus de certification et d'accréditation décrit les étapes que doivent suivre les divers intervenants pour exploiter une application opérationnelle gérée par des ressources internes ou par un tiers. Il est important de disposer de processus documentés de certification et d'accréditation qui ont été acceptés par les accréditeurs, puisque ces derniers sont responsables de l'acceptation du risque lié à l'exploitation de l'application opérationnelle. De plus, les accréditeurs assument les coûts liés à l'élaboration des livrables de certification nécessaires. Nous nous attendions à ce que les accréditeurs aient acceptés un processus documenté pour la certification et l'accréditation des nouvelles applications opérationnelles de TPSGC.

39. Nous avons constaté qu'aucun processus de certification et d'accréditation élaboré n'a été accepté par les accréditeurs ou par un comité composé de représentants de tous les accréditeurs, comme le Comité directeur de la Gestion de l'information-Technologie de l'information ministérielle.

40. Les accréditeurs peuvent ne pas comprendre quel processus de certification et d'accréditation à suivre, ni les livrables de certification ou les raisons pour lesquelles ceux-ci doivent être fournis. Un processus accepté de certification et d'accréditation aiderait les accréditeurs à planifier les ressources humaines et financières dont ils ont besoin pour obtenir l'accréditation de leurs applications opérationnelles. Il aiderait également l'autorité de certification dans l'exécution de ses fonctions lorsqu'il assure la liaison avec le personnel chargé d'élaborer les preuves de certification exigées.

La certification et l'accréditation des nouvelles applications opérationnelles de TPSGC se poursuivent

41. Un processus de certification et d'accréditation précise les livrables à fournir. Afin de réduire les coûts au minimum, il est important que le processus de certification et d'accréditation exige uniquement la création des livrables nécessaires pour la réalisation réussie de la certification et de l'accréditation. Nous nous attendions à ce que les livrables de certification exigés dans le cadre du processus suivi aient été produits pour les nouvelles applications opérationnelles certifiées et accréditées depuis avril 2007.

42. Nous avons examiné 17 nouvelles applications opérationnelles qui avaient été pleinement accréditées ou qui avaient reçu une autorisation d'exploitation provisoire (une autorisation d'exploitation provisoire reçue à la suite des activités de certification et d'accréditation est plus précise que les autorisations d'exploitation provisoires initiales des applications opérationnelles existantes au début du projet de conformité de la GSTI). Nous avons constaté que 10 des 17 nouvelles applications opérationnelles qui ont été pleinement certifiées et accréditées ou qui ont reçu une autorisation d'exploitation provisoire depuis avril 2007 respectaient le Cadre de

gestion de la sécurité des applications des SGASOTI. Tous les livrables exigés ont été fournis pour seulement deux des dix applications opérationnelles pour lesquelles ce processus a été suivi. Aucun des trois processus n'a été suivi pour les sept autres applications opérationnelles. Il n'est pas clair s'il est nécessaire ou possible pour un accréditeur de fournir tous les livrables exigés étant donné que ces derniers ont été certifiés et accrédités même si certains livrables manquaient et qu'aucun des trois processus n'a été suivi pour sept applications opérationnelles.

Exécution de l'évaluation de la qualité des documents clés

43. Les documents clés, comme les énoncés de la nature délicate et les EMR, sont présentés à l'autorité de certification en vue de l'obtention de la certification des applications opérationnelles de TPSGC. Une évaluation de la qualité comprend un examen des documents présentés dans le but de s'assurer que les renseignements fournis sont complets et de qualité suffisante. Il est important d'évaluer la qualité des documents clés afin que l'autorité de certification dispose des renseignements nécessaires pour formuler la recommandation appropriée à l'égard de l'accréditation à l'accréditeur. Nous nous attendions à ce que l'autorité de certification évalue la qualité des documents clés présentés en vue de l'obtention de la certification.

44. Nous avons constaté que l'autorité de certification examinait les documents clés et déterminait les préoccupations et les problèmes liés aux quatre nouvelles applications opérationnelles et aux huit applications opérationnelles existantes pour lesquelles nous avons examiné le processus d'évaluation de la qualité. Les évaluations de la qualité des documents clés appuient le processus de certification et d'accréditation et portent la direction à croire que la certification et l'accréditation sont bien faites.

CONCLUSIONS

45. Globalement, nous pouvons conclure que le Ministère dispose de processus appropriés pour faire en sorte que les risques pour les applications opérationnelles soient atténués ou acceptés. Les rôles et les responsabilités relatifs à la certification et à l'accréditation sont définis et assignés, et il n'existe aucun cas où les rôles ne sont pas respectés. La majorité des applications opérationnelles existantes de TPSGC est actuellement exploitée dans le cadre d'autorisations d'exploitation provisoires. Il s'agit d'une pratique acceptable qui donne le temps aux responsables des directions générales de TPSGC, à titre d'accréditeurs pour leurs applications opérationnelles, de traiter les conditions particulières avant l'obtention de la certification et de l'accréditation complètes. L'approbation de ces autorisations d'exploitation provisoires permet aux responsables des directions générales de TPSGC d'être au courant des progrès réalisés pour obtenir la certification et l'accréditation complètes et d'attester leur acceptation des risques associés à leurs applications opérationnelles. Bien que des progrès aient été réalisés dans la connaissance des applications opérationnelles existantes, tous les risques n'ont pas encore été déterminés. TPSGC n'a pas élaboré les livrables de base de certification qui permettent de déterminer ces

risques, comme les énoncés de la nature délicate et les évaluations de la menace et des risques, pour bon nombre de ses applications opérationnelles existantes à risque moyen et faible. Le processus à suivre pour atteindre la certification et l'accréditation complètes est clair; par contre, les progrès dans l'obtention de celles-ci ont été lents. En outre, en dépit d'une exigence obligatoire de la norme de GSTI, des évaluations de la menace et des risques n'ont pas été exigées pour les applications opérationnelles existantes évaluées à faible risque.

46. Le processus de certification et d'accréditation du Ministère pour les nouvelles applications opérationnelles n'est pas clair puisqu'il existe trois documents d'orientation. Aucun des documents d'orientation n'a été accepté par les responsables des directions générales de TPSGC, qui sont responsables de l'acceptation du risque lié à l'exploitation de leurs applications opérationnelles. Malgré cela, la certification et l'accréditation des nouvelles applications opérationnelles sont en cours.

RÉPONSE DE LA GESTION

La Direction générale des services d'infotechnologie est en accord avec les deux recommandations du plan d'action de la gestion et nous avons préparé des mesures pour les aborder en conséquence.

RECOMMANDATIONS ET PLAN D'ACTION DE LA GESTION

Recommandation 1 : Le président-directeur général de la Direction générale des services d'infotechnologie devrait s'assurer que le processus de certification et d'accréditation des applications opérationnelles existantes de niveau de risque faible exige une évaluation de la menace et des risques, et que les exigences de cette évaluation reflètent le risque associé à l'application opérationnelle.

> **Plan d'action de gestion 1.1 :** Conformément à la politique sur la Gestion de la sécurité des technologies de l'information du Secrétariat du Conseil du Trésor, toutes les directions générales ont été soumises à un processus rigoureux qui visait à déterminer le degré d'exposition aux risques de leurs applications opérationnelles surannées. Les résultats de ce processus ont été répartis en trois catégories (risque faible, risque moyen et risque élevé) et enregistrés dans la fiche de sécurité pour les secteurs d'affaires. Les directions générales ont également présenté un énoncé de nature délicate pour chacune de leurs applications opérationnelles surannées à faible risque. De plus, la Direction de la sécurité de la TI, qui est l'autorité ministérielle responsable de la certification et de l'accréditation, a validé les résultats de l'énoncé de nature délicate afin de garantir qu'aucune autre tâche de gestion des risques liés à la sécurité ne soit nécessaire. La Direction générale des services d'infotechnologie consultera le Secrétariat du Conseil du Trésor afin de s'assurer que les processus liés à la fiche de sécurité pour les secteurs d'affaires, à l'énoncé de nature délicate ainsi que la validation de la certification de la Direction de la sécurité de la TI sont conformes à l'article

12.3.2 de la norme opérationnelle de gestion de la sécurité des technologies de l'information en ce qui a trait à l'évaluation des menaces et des risques des applications opérationnelles surannées à risque faible, avant le 31 mars 2010.

Plan d'action de gestion 1.2 Si le Conseil du Trésor du Canada rejette le point 1, les directions générales devront effectuer une évaluation de la menace et des risques pour leurs applications opérationnelles surannées à faible risque avant le 30 avril 2010.

Recommandation 2 : Le président-directeur général de la Direction générale des services d'infotechnologie devrait clarifier qu'il existe un processus de certification et d'accréditation commun pour toutes les nouvelles applications opérationnelles de TPSGC, qui serait tout à fait conforme aux instruments de politique obligatoires applicables du gouvernement du Canada. Ce processus devrait être accepté par les responsables des directions générales de TPSGC, approuvé par le président-directeur général de la Direction générale des services d'infotechnologie et communiqué aux directions générales de TPSGC.

Plan d'action de gestion 2.1 : À TPSGC, l'Office du dirigeant principal de l'information détient l'autorité ministérielle sur le processus de la certification et l'accréditation. Le document intitulé « Cadre de travail sur la sécurité des applications » daté septembre 2008 est le processus utilisé par la Direction générale des services d'infotechnologie pour les nouveaux développements. Il sera présenté au comité directeur de la gestion de l'information et technologie de l'information pour acceptation comme norme ministérielle avant le 31 mars 2010.

À PROPOS DE LA VÉRIFICATION

Autorité

La présente vérification a été approuvée par le Comité de vérification, d'assurance et d'éthique de Travaux publics et Services gouvernementaux Canada en septembre 2006 dans le cadre du plan proposé d'assurance de la vérification interne.

Objectif

La présente vérification interne visait à évaluer la qualité des processus en place pour assurer l'atténuation ou l'acceptation par un niveau approprié de la direction, des menaces et des risques identifiés en relation avec les applications opérationnelles de TPSGC, avant que leur utilisation ne soit autorisée.

Étendue et méthode

La présente vérification couvrait la période d'octobre 2007 à novembre 2009.

La vérification était axée sur le processus de certification et d'accréditation en place pour garantir que les menaces et les risques de sécurité relevés en relation avec les applications opérationnelles de TPSGC soient atténués par des mesures appropriées, ou acceptés par un niveau de direction concerné, avant que leur utilisation ne soit autorisée.

La portée de la vérification englobait les applications opérationnelles existantes et nouvelles de TPSGC, les activités et l'orientation en matière de certification et d'accréditation relatives à ces applications opérationnelles, et les rapports sur les objectifs de certification et d'accréditation des applications opérationnelles, compris dans l'initiative de conformité de la GSTI de TPSGC.

La vérification ne portait pas sur les processus de certification et d'accréditation pour l'infrastructure des services partagés de technologie de l'information, dont TPSGC assume la gestion en tant que fournisseur de services partagés de technologie de l'information aux ministères, y compris à TPSGC.

Cette vérification a été réalisée conformément aux normes internationales pour la pratique professionnelle de la vérification interne.

En se fondant sur l'analyse des données et des preuves recueillies, l'équipe de vérification a préparé les constatations et les conclusions de la vérification, lesquelles ont été validées auprès des gestionnaires appropriés. Le rapport a ensuite été présenté au président-directeur général de la Direction générale des services d'infotechnologie pour son acceptation, et il sera déposé au Comité de vérification et d'évaluation en vue de l'obtention d'une recommandation d'approbation par le sous-ministre.

Critères

Les critères utilisés se fondaient principalement sur le Guide de vérification de la sécurité des technologies de l'information du Secrétariat du Conseil du Trésor du Canada et sur la norme de gestion de la sécurité des technologies de l'information (GSTI).

Les critères étaient les suivants :

- Les rôles, responsabilités et imputabilités à l'égard de la sécurité pour les applications opérationnelles de TPSGC ont été définis et assignés, et ils sont respectés;

- Des processus appropriés sont en place qui permettent de déterminer les applications de TI devant faire l'objet d'évaluations de la menace et des risques (EMR) et d'assurer qu'elles sont effectuées selon le niveau de risque et de priorité afin de satisfaire aux exigences relatives à la certification et à l'accréditation;

- Le processus de certification et d'accréditation assure que les menaces et les risques identifiés dans les EMR ont été atténués, ou acceptés par un niveau approprié de la direction, et que ces menaces et ces risques ont été communiqués de façon appropriée à la direction du Ministère et aux organismes centraux avant que l'utilisation des applications ne soit autorisée;

- Le processus de certification et d'accréditation donne lieu à une évaluation de la qualité des documents clés pertinents;

- Les rapports appropriés sont établis en ce qui a trait à l'état d'avancement du processus de certification et d'accréditation des applications opérationnelles relatives à l'initiative de conformité de la GSTI.

Fin des travaux de vérification

Les travaux de vérification sur le terrain pour la présente vérification ont été essentiellement achevés en juin 2008. Des documents additionnels ont été obtenus entre février 2009 et avril 2009, et entre octobre 2009 et novembre 2009. Ces mesures étaient nécessaires pour déterminer les progrès de TPSGC dans ses efforts pour obtenir la certification et l'accréditation de ses applications opérationnelles existantes, et pour déterminer le processus utilisé en vue de la certification des nouvelles applications opérationnelles.

Équipe de vérification

La vérification a été effectuée par des membres du Bureau de la vérification et de l'évaluation, sous la supervision du directeur, Vérification de l'infotechnologie, et sous la direction générale de la dirigeante principale de la vérification et de l'évaluation.

La vérification a été passée en revue par la fonction d'évaluation de la qualité du Bureau de la vérification et de l'évaluation.

ANNEXE A – INFORMATION SENSIBLE

L'information sensible doit être clairement identifiée en tant que telle. La nature délicate des renseignements est déterminée en fonction du préjudice éventuel que pourrait causer la divulgation non autorisée des renseignements, tel qu'il est défini dans la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels*.

Les renseignements pouvant porter préjudice à l'intérêt national sont des renseignements classifiés.

- La classification « Très secret » s'applique aux renseignements pouvant causer un préjudice exceptionnellement grave à l'intérêt national.
- La classification « Secret » s'applique aux renseignements pouvant causer un préjudice sérieux à l'intérêt national.
- La classification « Confidentiel » s'applique aux renseignements pouvant porter préjudice à l'intérêt national.

Les renseignements pouvant porter préjudice à des intérêts privés et à d'autres intérêts non nationaux sont des renseignements protégés.

- Les renseignements « Protégé C » sont des renseignements pouvant causer un préjudice extrêmement grave à des intérêts privés et à d'autres intérêts non nationaux.
- Les renseignements « Protégé B » sont des renseignements pouvant causer un préjudice sérieux à des intérêts privés et à d'autres intérêts non nationaux.
- Les renseignements « Protégé A » sont des renseignements pouvant porter préjudice à des intérêts privés et à d'autres intérêts non nationaux.