Rapport final

2007-723

Vérification de la gestion des accès pour certains systèmes d'infotechnologie sélectionnés

Bureau de la vérification et de l'évaluation

19 mars 2009

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

Table des matières

POINTS PRINCIPAUX

Points examinés

i. La gestion des accès vise à garantir que seules les personnes autorisées peuvent accéder aux ressources d'infotechnologie et aux renseignements selon le principe de l'accès sélectif[1]. De telles personnes devraient avoir une côte de sécurité appropriée et faire l'objet d'une authentification avant d'avoir accès aux ressources d'infotechnologie et aux renseignements.

ii. La vérification a examiné la gestion des accès pour deux systèmes de Technologie de l'information (TI) utilisés par le Bureau de la traduction pour la traduction de renseignements classifiés, et pour le Système de gestion des ressources humaines (SGRH) utilisé par la Direction générale des ressources humaines pour gérer les renseignements sur les employés et sur les postes pour le compte du ministère.

Importance

iii. La gestion des accès est un élément important de la sécurité des TI. Limiter l'accès aux systèmes de TI et aux renseignements qu'ils contiennent est particulièrement important lorsque l'information est sensible.

iv. Selon le niveau de confidentialité, l'accès non autorisé à des renseignements classifiés ou protégés stockés dans les systèmes de TI de TPSGC pourrait entraîner une perte de réputation ou un préjudice pour le ministère et pour ses clients, pour le gouvernement ou même pour le public canadien.

Constatations

v. Les mots de passe sont l'une des principales mesures de contrôle utilisées pour gérer l'accès aux systèmes de TI. Les Normes de sécurité de TPSGC concernant la TI comprennent des règles de composition des mots de passe, mais les règles en la matière ne sont toutefois pas toutes présentées comme étant obligatoires. D'autres lignes directrices émises par le ministère ne sont pas conformes aux Normes de sécurité de TPSGC concernant la TI. Cependant, les Normes de sécurité de TPSGC concernant la TI sont en cours de révision depuis le mois de septembre 2008.

vi. Il y a des applications d'infotechnologie, telles que celle utilisée par les employés de TPSGC pour se connecter à leur station de travail ou celle pour accéder à Internet, qui ne requièrent pas l'utilisation des règles de composition des mots de passe énoncées dans les Normes de sécurité de TPSGC concernant la TI.

[1] L'accès sélectif est défini comme étant la nécessité pour une personne d'accéder à des renseignements et de les connaître pour exécuter ses tâches.

vii. Le Bureau de la traduction a mis en œuvre certaines mesures en vue de contrôler l'accès aux systèmes utilisés pour la traduction de renseignements classifiés. Cependant, les processus et les procédures servant à gérer l'accès aux systèmes de TI n'étaient pas entièrement documentés. Certains contrôles manquaient, tels que le contrôle d'accès logique et l'approbation officielle de la direction pour la création et la modification des comptes d'utilisateur. Les systèmes n'étaient pas certifiés et accrédités tel qu'exigé par la *Politique du gouvernement sur la sécurité (PGS*). Cependant, le Bureau de la traduction a pris certaines mesures pour obtenir la certification et l'accréditation requises.

viii. La Direction générale des ressources humaines a des contrôles en place pour limiter l'accès au Système de gestion des ressources humaines (SGRH). Deux recommandations antérieures concernant la gestion des accès n'ont toutefois pas été mises en œuvre.

Recommandations et plan d'action de la direction

Réponse de la direction

La Direction générale des services d'infotechnologie considère que les résultats de la vérification reflètent de façon juste et exacte les directives sur l'utilisation des mots de passe à Travaux publics et Services gouvernementaux Canada. La Direction générale des services d'infotechnologie a l'intention d'agir suite aux recommandations de la vérification en mettant en place le plan d'action de la gestion décrit plus-bas.

Le Président-directeur général de la Direction générale des services d'infotechnologie devrait:

1. Mettre à jour les instruments de politique sur la sécurité de l'infotechnologie et les conseils aux usagers de Travaux publics et Services gouvernementaux Canada afin de garantir leur uniformité.

   Réponse de la Direction générale des services d'infotechnologie. La Direction générale des services d'infotechnologie accepte la recommandation et prendra les mesures suivantes **:**

   1.1 La Direction générale des services d'infotechnologie identifiera les instruments et les directives destinées à l'utilisateur relatifs à la politique de sécurité de la technologie de l'information (TI) de Travaux publics et Services gouvernementaux Canada (TPSGC), touchés par la présente vérification. Cette action sera complétée le 30 mars 2009.
   1.2 La Direction générale des services d'infotechnologie validera l'information pour garantir la cohérence et mettre à jour les instruments de politique et les

directives destinées à l'utilisateur, s'il y a lieu. Cette action sera complétée le 30 juin 2009.

1.3 La Direction générale des services d'infotechnologie fera approuver par le Ministère les instruments de politique qui doivent être mis à jour le cas échéant. Cette action sera complétée le 30 juin 2009.

2. Mettre à jour les Normes de sécurité de Travaux publics et Services gouvernementaux Canada concernant la TI afin d'assurer que les règles s'appliquant aux mots de passe reflètent les risques inhérents, sont basées sur des critères spécifiques, et sont énoncées comme des conditions obligatoires.

Réponse de la Direction générale des services d'infotechnologie. La Direction générale des services d'infotechnologie accepte la recommandation et prendra les mesures suivantes :

2.1 La Direction générale des services d'infotechnologie révisera les règles régissant les mots de passe énoncées dans le document Normes de sécurité de TPSGC concernant la TI en tenant compte des risques inhérents et présentera les règles régissant les mots de passe comme des exigences obligatoires. L'entrée en vigueur des règles de mots de passe révisées tiendra compte des risques inhérents. Cette action sera complétée le 30 juin 2009.

2.2 Faire approuver par le Ministère les règles de mots de passe des Normes de la sécurité des TI. Cette action sera complétée le 30 septembre 2009.

2.3 Publier les documents des normes de sécurité relatifs aux règles de mots de passe. Cette action sera complétée le 30 novembre 2009.

3. Appliquer les Normes de sécurité de Travaux publics et Services gouvernementaux Canada à l'ensemble des systèmes et des applications de Travaux publics et Services gouvernementaux Canada gérés par la Direction générale des services d'infotechnologie.

Réponse de la Direction générale des services d'infotechnologie. La Direction générale des services d'infotechnologie accepte la recommandation et prendra les mesures suivantes **:**

3.1 La Direction générale des services d'infotechnologie mènera une analyse des écarts afin d'évaluer la portée des modifications nécessaires à l'application des règles de mots de passe révisées. Cette action sera complétée le 30 août 2009.

3.2 La Direction générale des services d'infotechnologie préparera une demande motivée et la présentera au chef des finances en vue d'obtenir l'approbation du Ministère en ce qui concerne l'approche la plus appropriée et présentant le meilleur rapport coût-efficacité pour l'application des nouvelles règles de mots de passe. Cette action sera complétée le 30 septembre 2009.

3.3 Lorsque l'approche présentant le meilleur rapport coût-efficacité en ce qui concerne l'application des nouvelles règles de mots de passe sera approuvée, la Direction générale des services d'infotechnologie appliquera les nouvelles règles de mots de passe, en fonction des fonds approuvés. Cette action sera complétée le 31 décembre 2010.
3.4 Le secteur de la Gestion et prestation des services et le secteur de la Gestion des applications et des services opérationnels des TI ainsi que les directions générales de TPSGC feront périodiquement état de leur conformité au Bureau du dirigeant principal de l'information. Le Bureau du dirigeant principal de l'information rendra compte périodiquement de l'état de conformité au Comité directeur de la gestion de l'information et de la technologie de l'information ministérielle. Cette action sera complétée le 30 novembre 2009.

Réponse de la direction

Le Bureau de la traduction considère que les résultats de la vérification reflètent de façon juste et exacte l'état du cadre de contrôle de la gestion en place visant à protéger les systèmes d'infotechnologie utilisés pour le soutien à la traduction de renseignements classifiés contre l'accès non autorisé. Le Bureau de la traduction a l'intention d'agir suite aux recommandations de la vérification en mettant en place le plan d'action de la gestion décrit plus-bas.

La Présidente-directrice générale du Bureau de la traduction devrait :

1. Documenter, approuver et mettre en œuvre des processus et des procédures de soutien pour la gestion des accès pour tous les points de service où des systèmes d'infotechnologie appartenant à Travaux publics et Services gouvernementaux Canada sont utilisés pour le soutien à la traduction de renseignements classifiés. De tels processus devraient être conformes aux instruments de politique du Secrétariat du Conseil du Trésor du Canada en matière de sécurité et aux politiques ministérielles.

   Réponse du Bureau de la traduction. Le Bureau de la traduction accepte la recommandation et prendra les mesures suivantes :

   Livrable : directive (processus et procédures).

   1.1 Identification des éléments manquants au cadre et procédures existants du Bureau de la traduction. Cette action sera complétée en mars 2009.
   1.2 Finalisation du livrable. Cette action sera complétée en mai 2009.
   1.3 Validation du livrable. Cette action sera complétée en juillet 2009.
   1.4 Élaboration d'un plan de communication. Cette action sera complétée en mai 2009.
   1.5 Approbation finale par la Présidente-Directrice générale du Bureau de la traduction. Cette action sera complétée en août 2009.

1.6 Exécution du plan de communication. Cette action sera complétée en août 2009.

2. Élaborer un processus pour régir la destruction des renseignements classifiés confiés au Bureau de la traduction et traités sur des systèmes appartenant à Travaux publics et Services gouvernementaux Canada.

   Réponse du Bureau de la traduction. Le Bureau de la traduction accepte la recommandation et prendra les mesures suivantes :

   Livrable : directive (processus et procédures).

   2.1 Identification des éléments manquants au cadre et procédures existants du Bureau de la traduction. Cette action sera complétée en mars 2009.
   2.2 Finalisation du livrable. Cette action sera complétée en mai 2009.
   2.3 Validation du livrable. Cette action sera complétée en juillet 2009.
   2.4 Élaboration d'un plan de communication. Cette action sera complétée en mai 2009.
   2.5 Approbation finale par la Présidente-Directrice générale du Bureau de la traduction. Cette action sera complétée en août 2009.
   2.6 Exécution du plan de communication. Cette action sera complétée en août 2009.

3. Certifier et accréditer les systèmes appartenant à Travaux publics et Services gouvernementaux Canada utilisés par le personnel du Bureau de traduction pour le soutien à la traduction de renseignements classifiés.

   Réponse du Bureau de la traduction. Le Bureau de la traduction accepte la recommandation et prendra les mesures suivantes :

   Livrable : Certification et accréditation des solutions technologiques-types de traitement des renseignements classifiés du Bureau de la traduction.

   3.1 Revue des actions à compléter dans le cadre du processus de certification en cours avec la Direction de la sécurité de la technologie de l'information. Cette action sera complétée en avril 2009.
   3.2 Compléter toutes les étapes du processus normalisé de certification et d'accréditation des solutions technologiques-types de traitement des renseignements classifiés du Bureau de la traduction;
      3.2.1 Confirmation du processus de certification et d'accréditation selon le niveau d'effort. Cette action sera complétée en avril 2009.
      3.2.2 Confirmation du plan de certification auprès de la Direction de la sécurité de la technologie de l'information. Cette action sera complétée en mai 2009.

3.2.3 Énoncé des risques acceptables. Cette action sera complétée en juillet 2009.
3.2.4 Validation de l'architecture/la conception auprès de la Direction de la sécurité de la technologie de l'information. Cette action sera complétée en octobre 2009.
3.2.5 Validation des exigences de la sécurité auprès de la Direction de la sécurité de la technologie de l'information. Cette action sera complétée en février 2009.
3.2.6 Rapport sur les éléments probants de la certification. Cette action sera complétée en avril 2010.
3.2.7 Lettre de certification émise par l'autorité de certification des systèmes et applications du Bureau de la traduction, en l'occurrence le directeur, direction de la sécurité de la technologie de l'information du Bureau du DPI au sein de la direction générale des services d'infotechnologie. Cette action sera complétée en juin 2010.

3.3 Approbation finale de la lettre d'accréditation par l'autorité d'accréditation des systèmes et applications du Bureau de la traduction, en l'occurrence la Présidente-Directrice générale du Bureau de la traduction. Cette action sera complétée en juin 2010.

Réponse de la direction

La Direction générale des ressources humaines considère que les résultats de la vérification reflètent de façon juste et exacte l'état du cadre de contrôle de la gestion visant à protéger le Système de gestion des ressources humaines contre l'accès non autorisé. La Direction générale des ressources humaines a l'intention d'agir suite aux recommandations de la vérification, en mettant en place le plan d'action de la gestion décrit plus-bas.

La sous-ministre adjointe de la Direction générale des ressources humaines devrait :

1. Répondre à toutes les recommandations en suspens relativement à la gestion des accès contenues dans l'évaluation de la menace et des risques datée du 2007-12-20.

   Réponse de la Direction générale des ressources humaines. La Direction générale des ressources humaines accepte la recommandation et prendra les mesures suivantes :

   1.1 Afin d'adresser la première recommandation de menace et des risques (Considérer le cryptage de transfert de données pour améliorer la sécurité), la direction générale des ressources humaines conclura un accord écrit avec la direction générale des services d'infotechnologie pour s'assurer que des données protégées de B transmises entre le système de gestion des ressources

humaines et d'autres systèmes de TPSGC sont cryptées. Cette action sera complétée le 31 mars 2009.

1.2 La direction générale des ressources humaines fera le suivi sur les progrès par rapport à l'accord jusqu'à ce que toutes les interfaces entre le système de gestion des ressources humaines et d'autres systèmes de TPSGC, et entre les deux composantes identifiées dans l'évaluation de la menace et des risques, soient modifiées pour s'assurer que les données protégées B transmises sont cryptées. Cette action sera complétée le 31 mars 2010

1.3 À l'automne 2008, l'intention était de migrer à PeopleSoft, y compris toutes les données historiques du système de gestion des ressources humaines. Cependant, en raison du manque de fonds, le projet a été retardé et, la décision de ne pas migrer toutes les données historiques a été prise basée sur une approche plus efficace et moins onéreuse. Par conséquent, pour adresser la deuxième recommandation de l'évaluation de la menace et des risques liée à la gestion d'accès (considérer le déplacement vers un environnement protégé plus approprié), la direction générale des ressources humaines conclura un accord écrit avec la direction générale des services d’infotechnologie pour s'assurer que le système de gestion des ressources humaines est logé dans un environnement approprié contrôlé par la direction générale des services d’infotechnologie. Cette action sera complétée le 30 juin 2009.

1.4 La direction générale des ressources humaines fera le suivi sur les progrès par rapport à l'accord jusqu'à ce que les travaux exigés, pour loger le système de gestion des ressources humaines dans un environnement approprié, soient terminés. Cette action sera complétée le 31 mars 2011.

INTRODUCTION

1. La gestion des accès vise à garantir que seules les personnes autorisées peuvent accéder aux renseignements et aux ressources d'infotechnologie selon le principe de l'accès sélectif. De telles personnes devraient avoir une côte de sécurité appropriée et faire l'objet d'une authentification avant d'avoir accès aux renseignements et aux ressources d'infotechnologie.

2. La *Politique du gouvernement sur la sécurité (PGS)* de 2002 a comme objectif de protéger les employés; de préserver la confidentialité, l'intégrité, la disponibilité et la valeur des biens; et de garantir la prestation continue des services. Étant donné que le gouvernement du Canada se fie largement aux technologies de l'information (TI) pour fournir ses services, cette politique souligne la nécessité pour les ministères de surveiller leurs activités électroniques.

3. La norme Gestion de la sécurité des technologies de l'information (GSTI) soutient la PGS en définissant les exigences de base en matière de sécurité que les ministères fédéraux doivent satisfaire pour assurer la sécurité de l'information et des biens TI sous leur contrôle. La GSTI fournit une orientation quant à l'organisation et à la gestion de la sécurité des TI au sein des ministères, y compris une description des contrôles de gestion, ainsi que des mesures de protection techniques et opérationnelles qui soutiennent de tels contrôles.

4. Les principales politiques et normes ministérielles traitant de la gestion des accès en matière de TI sont les suivantes :

    - Politique ministérielle (PM) 055 – Programme de sécurité de la technologie de l'information (TI)
    - PM 029 – Les employés qui quittent TPSGC
    - Normes de sécurité de TPSGC concernant la TI

5. Travaux publics et Services gouvernementaux Canada (TPSGC) gère plus de 400 applications d'affaires et systèmes de soutien. Plusieurs de ces systèmes stockent et traitent des renseignements sensibles. En se fondant sur une analyse des risques, trois de ces systèmes ont été choisis pour la présente vérification : deux systèmes utilisés par le Bureau de la traduction pour le soutien à la traduction de documents classifiés ainsi que le Système de gestion des ressources humaines (SGRH).

6. Le Bureau de la traduction fournit des services à ses clients au moyen de quelque 60 points de service situés dans la région de la capitale nationale et à la grandeur du Canada. La vérification a examiné deux systèmes différents utilisés par le Bureau de la traduction pour le soutien à la traduction de documents classifiés dans deux points de service. Dans le présent rapport, ces systèmes sont désignés par l'appellation « solutions de traitement de documents secrets » ou « solutions », et les deux points

de service examinés par la vérification sont désignés par l'appellation point de service A et point de service B. Les solutions utilisées dans les points de service dépendent d'ordinateurs personnels qui ne sont pas connectés à Internet ni à l'intranet de TPSGC. Les conclusions tirées à partir des systèmes examinés ne peuvent être appliquées aux autres systèmes étant donné que différents points de service utilisent différents systèmes. Le Bureau de la traduction a toutefois l'intention de déployer la solution examinée pour le point de service A dans les autres points de service où sont traduits des renseignements classifiés.

7. Le Système de gestion des ressources humaines (SGRH) est utilisé par la Direction générale des ressources humaines pour gérer les renseignements sur les employés et les postes pour le compte de TPSGC. Ces renseignements servent à soutenir les fonctions des ressources humaines, telles que la classification, la rémunération, l'évaluation du rendement, la dotation en personnel, les langues officielles, les rajustements d'effectifs et l'équité en matière d'emploi. Le SGRH fonctionne sur l'infrastructure de services partagés de TI (SPTI), qui est gérée par la Direction générale des services d'infotechnologie (DGSIT).

OBJECTIFS DE LA VÉRIFICATION

8. L'objectif de cette vérification interne était de déterminer si le cadre de contrôle de la gestion servant à protéger contre l'accès non autorisé à certains systèmes d'infotechnologie sélectionnés était suffisant. Plus précisément, cette vérification avait pour objectif d'évaluer si des mesures appropriées étaient en place afin de contrôler et limiter l'accès aux systèmes et aux renseignements sensibles, en limitant l'accès aux personnes qui détiennent une approbation officielle, la côte de sécurité requise et ont un accès sélectif.

9. La vérification consistait à examiner la gestion des accès pour trois systèmes : deux systèmes utilisés par le Bureau de la traduction pour le soutien à la traduction de documents classifiés dans deux points de service et le Système de gestion des ressources humaines (SGRH).

10. La vérification n'a pas examiné la sécurité physique des systèmes ni la sécurité de l'infrastructure de services partagés de TI.

11. D'autres renseignements sur les objectifs, la portée, l'approche et les critères de la vérification se trouvent dans la section « À propos de la vérification » à la fin du rapport.

OBSERVATIONS

NORMES DE SÉCURITÉ DE TPSGC CONCERNANT LA TI

Les lignes directrices sur l'utilisation des mots de passe ne sont pas uniformes et elles ne sont pas appliquées

12. Les mots de passe sont l'une des principales mesures de contrôle utilisées pour gérer l'accès aux systèmes de TI. Ils visent à garantir que l'accès aux applications et aux systèmes de soutien n'est accordé qu'aux personnes autorisées. Les règles de composition des mots de passe dictent le nombre et le type de caractères requis pour des mots de passe donnés. Plus un mot de passe est complexe, moins il y a de risques qu'il soit contourné.

13. L'équipe de vérification s'attendait à ce que le ministère ait des règles de composition des mots de passe claires, uniformes et obligatoires, soutenues par des systèmes et des applications ministérielles, et conformes à la PGS.

14. L'équipe de vérification a constaté que l'une des règles de composition des mots de passe des Normes de sécurité de TPSGC concernant la TI était présentée comme étant une bonne pratique et non pas comme une prescription. En outre, il existe des contradictions dans l'orientation fournie sur l'intranet de TPSGC quant aux exigences en matière de mots de passe. Bien que les Normes de sécurité de TPSGC concernant la TI stipulent que la « longueur minimale d'un mot de passe est de huit caractères », plusieurs autres documents de TPSGC ne sont pas conformes à ces normes de sécurité. Ils incluent notamment le cours de sensibilisation à la sécurité de l'infotechnologie de TPSGC et les documents de sensibilisation à la sécurité, qui indiquent que la longueur minimale d'un mot de passe est de six caractères.

15. Les règles de composition des mots de passe en vigueur pour les applications utilisées par les employés de TPSGC pour accéder à Novell (accès au réseau), à Outlook (courriel), à Internet et au SGRH, n'appliquent pas les Normes de sécurité de TPSGC concernant la TI.

16. En l'absence de règles sur les mots de passe claires, uniformes et appliquées par les systèmes et les applications de TPSGC, il y a un risque d'accès non autorisé aux renseignements qu'ils protègent.

SYSTÈMES CLASSIFIÉS UTILISÉS PAR LE BUREAU DE LA TRADUCTION

17. Un cadre de contrôle de gestion vise à garantir que l'organisation atteint ses objectifs. On s'attend à ce que le cadre de contrôle de la gestion destiné à protéger les systèmes de TI contre les accès non autorisés garantisse que l'accès est limité aux personnes

qui ont une côte de sécurité appropriée, qui ont été authentifiées et autorisées, et qui nécessitent l'accès aux renseignements.

18. Pour atteindre ces objectifs, le cadre de contrôle de la gestion doit comprendre de multiples contrôles : les lignes directrices sur le contrôle des accès doivent se conformer à la PGS, et de la documentation connexe doit avoir été élaborée, disséminée et tenue à jour; un gestionnaire bien renseigné et responsable doit approuver officiellement l'accès aux renseignements ou à des biens de nature délicate aux personnes qui en ont besoin en vertu du principe d'« accès sélectif »; l'accès doit être limité aux personnes ayant une côte de sécurité appropriée; des mesures d'identification et d'authentification des utilisateurs doivent être intégrées aux applications et aux systèmes de soutien; les privilèges d'accès doivent être tenus à jour; la séparation des responsabilités doit être reflétée dans les privilèges d'accès; et des processus doivent être en place pour traiter des accès non autorisés.

19. Nous avons constaté que les contrôles mentionnés ci-dessus n'étaient pas uniformément appliqués par le Bureau de la traduction dans les deux points de service examinés pour protéger contre les accès non autorisés aux systèmes utilisés pour le soutien à la traduction de renseignements classifiés. Plusieurs contrôles étaient toutefois en place, particulièrement en ce qui concerne le point de service A. Dans ce cas, les privilèges d'accès étaient à jour. Les procédures pour révoquer l'accès logique n'étaient cependant que partiellement documentées. La séparation des tâches était mise en œuvre grâce à une séparation des rôles et les procédures pour traiter des accès non autorisés avaient été documentées. En ce qui concerne le point de service B, aucun accès logique aux systèmes de TI n'avait été mis en œuvre.

Processus et procédures non entièrement documentés

20. Un processus décrit ce qu'il faut faire (p. ex., la création d'un compte d'utilisateur), tandis qu'une procédure explique comment le faire. Les exigences stipulées dans un processus peuvent être satisfaites selon une ou plusieurs procédures. Les contrôles sont toute mesure prise par la direction et par d'autres parties pour gérer les risques et pour accroître les chances d'atteindre les objectifs fixés.

21. En documentant les processus et les contrôles qui y sont associés, la direction peut les communiquer et en assurer la compréhension commune par toutes les personnes concernées. Cela contribue à garantir une exécution et un contrôle constants des activités, même lorsque les personnes qui en sont responsables changent. Des processus dûment documentés peuvent aussi aider les personnes concernées à mieux comprendre le contexte entourant des activités et des contrôles particuliers, et leur fournir ainsi des renseignements pour prendre les décisions appropriées.

22. Nous nous attendions à trouver des processus et des procédures documentés pour soutenir la gestion des accès aux solutions de traitement de documents secrets

utilisées par le Bureau de la traduction dans ses points de service. Pour contrôler l'accès à ces solutions, nous nous attendions à ce que les gestionnaires responsables approuvent la création et la modification des comptes d'utilisateurs des personnes ayant une côte de sécurité appropriée et selon un principe d'« accès sélectif ».

23. Nous avons constaté que les solutions de traitement de documents secrets utilisées dans les deux points de service examinés étaient très différentes. En outre, l'accès à ces solutions était également géré de manière différente. Bien que les systèmes du point de service B soient conservés dans une salle sécurisée, des contrôles de l'accès logique, tels que des noms d'utilisateur et des mots de passe, n'avaient pas été mis en œuvre. La GSTI requiert que des mesures d'identification et d'authentification soient incorporées à tous les systèmes. De plus, il a été déterminé que sur un échantillon de 107 personnes qui avaient accès à la salle sécurisée, 10 n'avaient pas la côte de sécurité requise.

24. Au point de service A, même si le contrôle de l'accès logique avait été mis en œuvre, que les utilisateurs possédaient les autorisations de sécurité appropriées et que la solution était soutenue par un certain nombre de procédures documentées, les processus globaux pour créer, modifier et révoquer les comptes n'étaient pas entièrement documentés. De plus, les procédures pour soutenir la révision régulière des comptes et pour assurer l'identification appropriée des personnes à qui des identificateurs uniques étaient émis, n'étaient pas documentées.

25. Un certain nombre de contrôles relatifs à la gestion des accès sont soit manquants ou appliqués de manière inconstante dans le point de service A. Par exemple, le processus ne requiert pas qu'un gestionnaire bien renseigné et responsable approuve la création ou la modification des comptes d'utilisateur. Certains mots de passe n'expirent pas dans les délais stipulés par les Normes de sécurité de TPSGC concernant la TI. Dans deux cas, un compte privilégié (nom d'utilisateur et mot de passe) était partagé par deux personnes. De tels comptes permettent aux personnes d'exécuter des activités sensibles comme les modifications de mots de passe. Lorsque de tels comptes sont partagés, il est possible que les opérations exécutées ne puissent être attribuées à une seule personne. Les Normes de sécurité de TPSGC concernant la TI stipulent que chaque utilisateur autorisé doit être identifié uniquement.

26. En raison de ces faiblesses, les activités et les contrôles qui soutiennent la gestion des accès ne sont pas toujours exécutés en conformité avec la PGS.

Absence de processus pour la destruction des renseignements classifiés

27. L'information est la pierre angulaire d'un gouvernement démocratique, efficace et imputable. Elle doit être bien gérée tout au long de son cycle de vie, y compris au moment de sa destruction. Nous nous attendions à ce que le Bureau de la traduction

ait mis en œuvre des processus appropriés ainsi que les procédures associées pour la conservation et la destruction des renseignements classifiés.

28. La procédure opérationnelle de traitement des documents secrets utilisée dans le point de service A décrit comment utiliser la solution de traitement des documents secrets pour traiter des renseignements classifiés. Elle guide les utilisateurs dans les différentes phases : la réception, la traduction, la révision et la correction, la livraison et le stockage. Cette procédure demande aux utilisateurs de sauvegarder leur document final dans un répertoire d'archivage. La procédure ne précise toutefois pas à quel moment il faut disposer des documents classifiés, qui est responsable de leur destruction, et comment ces activités sont contrôlées. L'information dans le répertoire est conservée pour une période indéterminée.

29. Comme il n'y a aucun processus en place pour la destruction des renseignements classifiés, ceux-ci demeurent dans le répertoire et ils ne sont ne sont pas détruits d'une manière conforme aux politiques. Comme avec le temps un volume important de renseignements classifiés peut s'accumuler à un endroit, le risque que TPSGC devienne la cible d'accès non autorisés est accrût et ainsi que l'impact que pourraient avoir un tel accès.

Les solutions de traitement de documents secrets n'ont pas été certifiées ni accréditées

30. La Politique du gouvernement sur la sécurité stipule que les ministères doivent certifier et accréditer leurs systèmes de TI avant de les exploiter. Le but de la certification est de vérifier que les exigences en matière de sécurité déterminées pour un système ou un service en particulier sont respectées et que les contrôles et les mesures de protection fonctionnent comme prévu. Le but de l'accréditation est de signifier que la direction a autorisé l'exploitation du système ou du service et qu'elle a accepté le risque résiduel qui en découle. L'accréditation est fondée sur le processus de certification ainsi que sur d'autres considérations de gestion.

31. Nous nous attendions à ce que les solutions de traitement des documents secrets dans les deux points de service aient été certifiées et accréditées. Ceci est particulièrement important parce que des renseignements classifiés jusqu'à un niveau secret sont traités au moyen de ces systèmes d'infotechnologie. En outre, le Bureau de la traduction a indiqué que son objectif était de dupliquer la solution mise en œuvre au point de service A dans les autres points de service où des renseignements classifiés sont traduits. Nous avons constaté que les systèmes de TI n'étaient pas certifiés et accrédités. Cependant, le Bureau de la traduction a pris certaines mesures pour obtenir la certification et l'accréditation requises.

32. Sans certification et accréditation, le Bureau de la traduction est incapable de démontrer que les contrôles de sécurité et les mesures de protection des systèmes sont

suffisants pour faire face aux risques d'un accès non autorisé à des renseignements classifiés.

SYSTÈME DE GESTION DES RESSOURCES HUMAINES (SGRH)

33. Nous avons constaté que le cadre de contrôle de la gestion des accès était généralement en place et adéquat pour protéger le SGRH contre les accès non autorisés. Dans le cadre de notre vérification, nous avons identifié deux secteurs d'amélioration. L'un de ces secteurs a déjà été adressé. L'importance et l'impact de ces observations, de même que la recommandation correspondante, sont décrits plus en détail dans les sections suivantes du présent rapport de vérification.

Deux recommandations antérieures concernant la gestion des accès n'ont pas été mises en œuvre

34. Les ministères doivent se conformer aux exigences de base de la PGS et ils doivent effectuer leur propre évaluation de la menace et des risques (EMR) pour déterminer la nécessité d'intégrer des exigences autres que celles stipulées par la PGS.

35. Nous nous attendions à ce que la Direction générale des ressources humaines ait pris les mesures appropriées pour s'assurer que le SGRH respecte les exigences de la PGS. Bien que la direction générale ait bel et bien effectué une EMR, elle ne s'est pas assurée que les deux recommandations relatives à la gestion des accès, dont la mise en œuvre relève de la DGSIT, avaient été suivies. Si la Direction générale des ressources humaines est responsable des deux risques associés aux deux recommandations de l'EMR, le premier est partagé avec d'autres Directions de TPSGC, étant donné que toutes les Directions de TPSGC utilisent l'infrastructure de services partagés de TI. Ce risque est atténué par la DGSIT dans le cadre de l'atteinte de la conformité à la GSTI pour l'infrastructure de services partagés de TI. Bien que la deuxième recommandation de l'EMR nécessitera que la DGSIT mette en œuvre une solution pour atténuer le risque, ce risque est propre à la Direction générale des ressources humaines. Le risque d'accès non autorisé aux renseignements du SGRH demeure étant donné que les recommandations de l'EMR n'ont pas été mises en œuvre.

Des identifications génériques des utilisateurs ont été utilisées pour des raisons opérationnelles

36. Une identification d'utilisateur générique est un nom d'utilisateur et un mot de passe partagés par deux personnes ou plus. On peut utiliser des identifications d'utilisateur génériques pour des raisons d'efficacité opérationnelle lorsque deux utilisateurs ou plus ont besoin d'une fonctionnalité particulière. Les identifications génériques pour utilisateurs multiples limitent la capacité d'imputer des actions à une personne en particulier et elles compliquent l'application du contrôle des accès au système.

L'utilisation d'identifications d'utilisateur génériques n'est pas conforme à la politique ministérielle 055 de TPSGC sur la sécurité de la technologie de l'information, qui indique qu'un identificateur d'utilisateur unique doit être attribué à chaque utilisateur avant que celui-ci n'ait accès aux systèmes et aux renseignements de TI. Ceci est important parce que cela permet d'attribuer les actions à une personne en particulier et facilite la gestion des accès.

37. Nous nous attendions à ce que chaque utilisateur du SGRH ait une identification d'utilisateur unique. L'équipe de vérification a constaté que quatre identifications d'utilisateur génériques sur environ 600 comptes étaient utilisées pour des raisons opérationnelles. Le SGRH a cessé d'utiliser toute identification d'utilisateur générique en juin 2008. Cette mesure a été attestée par l'équipe de vérification et c'est pour cette raison qu'aucune recommandation n'a été formulée relativement à cette observation.

CONCLUSIONS

38. Le cadre de contrôle de la gestion en place au moment de la vérification pour protéger contre les accès non autorisés aux systèmes de TI utilisés et détenus par le Bureau de la traduction, pour le soutien à la traduction de renseignements classifiés, n'était pas adéquat. Bien que certaines mesures étaient en place pour contrôler l'accès aux systèmes de TI, ces mesures n'étaient pas suffisantes pour limiter l'accès aux systèmes et aux renseignements classifiés aux personnes ayant la côte de sécurité requise, une approbation officielle et un accès sélectif.

39. Nous avons constaté que le cadre de contrôle de la gestion des accès était généralement en place et adéquat pour protéger contre les accès non autorisés au SGRH. Il y a toutefois deux recommandations découlant de l'EMR relatives à la gestion des accès qui doivent être mises en œuvre.

RECOMMANDATIONS ET PLAN D'ACTION DE LA DIRECTION

Réponse de la direction

40. La Direction générale des services d'infotechnologie considère que les résultats de la vérification reflètent de façon juste et exacte les directives sur l'utilisation des mots de passe à Travaux publics et Services gouvernementaux Canada. La Direction générale des services d'infotechnologie a l'intention d'agir suite aux recommandations de la vérification en mettant en place le plan d'action de la gestion décrit plus-bas.

41. Le Président-directeur général de la Direction générale des services d'infotechnologie devrait:

1. Mettre à jour les instruments de politique sur la sécurité de l'infotechnologie et les conseils aux usagers de Travaux publics et Services gouvernementaux Canada afin de garantir leur uniformité.

   Réponse de la Direction générale des services d'infotechnologie. La Direction générale des services d'infotechnologie accepte la recommandation et prendra les mesures suivantes **:**

   1.1 La Direction générale des services d'infotechnologie identifiera les instruments et les directives destinées à l'utilisateur relatifs à la politique de sécurité de la technologie de l'information (TI) de Travaux publics et Services gouvernementaux Canada (TPSGC), touchés par la présente vérification. Cette action sera complétée le 30 mars 2009.
   1.2 La Direction générale des services d'infotechnologie validera l'information pour garantir la cohérence et mettre à jour les instruments de politique et les directives destinées à l'utilisateur, s'il y a lieu. Cette action sera complétée le 30 juin 2009.
   1.3 La Direction générale des services d'infotechnologie fera approuver par le Ministère les instruments de politique qui doivent être mis à jour le cas échéant. Cette action sera complétée le 30 juin 2009

2. Mettre à jour les Normes de sécurité de Travaux publics et Services gouvernementaux Canada concernant la TI afin d'assurer que les règles s'appliquant aux mots de passe reflètent les risques inhérents, sont basées sur des critères spécifiques, et sont énoncées comme des exigences obligatoires.

   Réponse de la Direction générale des services d'infotechnologie. La Direction générale des services d'infotechnologie accepte la recommandation et prendra les mesures suivantes :

   2.1 La Direction générale des services d'infotechnologie révisera les règles régissant les mots de passe énoncées dans le document Normes de sécurité de TPSGC concernant la TI en tenant compte des risques inhérents et présentera les règles régissant les mots de passe comme des exigences obligatoires. L'entrée en vigueur des règles de mots de passe révisées tiendra compte des risques inhérents. Cette action sera complétée le 30 juin 2009.
   2.2 Faire approuver par le Ministère les règles de mots de passe des Normes de la sécurité des TI. Cette action sera complétée le 30 septembre 2009.
   2.3 Publier les documents des normes de sécurité relatifs aux règles de mots de passe. Cette action sera complétée le 30 novembre 2009.

3. Appliquer les Normes de sécurité de Travaux publics et Services gouvernementaux Canada à tous les systèmes et les applications de Travaux publics et Services gouvernementaux Canada gérés par la Direction générale des services d'infotechnologie.

   Réponse de la Direction générale des services d'infotechnologie. La Direction générale des services d'infotechnologie accepte la recommandation et prendra les mesures suivantes **:**

   3.1 La Direction générale des services d'infotechnologie mènera une analyse des écarts afin d'évaluer la portée des modifications nécessaires à l'application des règles de mots de passe révisées. Cette action sera complétée le 30 août 2009.
   3.2 La Direction générale des services d'infotechnologie préparera une demande motivée et la présentera au chef des finances en vue d'obtenir l'approbation du Ministère en ce qui concerne l'approche la plus appropriée et présentant le meilleur rapport coût-efficacité pour l'application des nouvelles règles de mots de passe. Cette action sera complétée le 30 septembre 2009.
   3.3 Lorsque l'approche présentant le meilleur rapport coût-efficacité en ce qui concerne l'application des nouvelles règles de mots de passe sera approuvée, la Direction générale des services d'infotechnologie appliquera les nouvelles règles de mots de passe, en fonction des fonds approuvés. Cette action sera complétée le 31 décembre 2010.
   3.4 Le secteur de la Gestion et prestation des services et le secteur de la Gestion des applications et des services opérationnels des TI ainsi que les directions générales de TPSGC feront périodiquement état de leur conformité au Bureau du dirigeant principal de l'information. Le Bureau du dirigeant principal de l'information rendra compte périodiquement de l'état de conformité au Comité directeur de la gestion de l'information et de la technologie de l'information ministérielle. Cette action sera complétée le 30 novembre 2009.

Réponse de la direction

42. Le Bureau de la traduction considère que les résultats de la vérification reflètent de façon juste et exacte l'état du cadre de contrôle de la gestion en place visant à protéger les systèmes d'infotechnologie utilisés pour le soutien à la traduction de renseignements classifiés contre l'accès non autorisé. Le Bureau de la traduction a l'intention d'agir suite aux recommandations de la vérification en mettant en place le plan d'action de la gestion décrit plus-bas.

43 La Présidente-directrice générale du Bureau de la traduction devrait :

1. Documenter, approuver et mettre en œuvre des processus et des procédures de soutien pour la gestion des accès pour tous les points de service où des systèmes d'infotechnologie appartenant à Travaux publics et Services gouvernementaux Canada sont utilisés pour le soutien à la traduction de renseignements classifiés. De tels processus devraient être conformes aux instruments de politique du Secrétariat du Conseil du Trésor du Canada en matière de sécurité et aux politiques ministérielles.

   Réponse du Bureau de la traduction. Le Bureau de la traduction accepte la recommandation et prendra les mesures suivantes :

   Livrable : directive (processus et procédures).

   1.1 Identification des éléments manquants au cadre et procédures existants du Bureau de la traduction. Cette action sera complétée en mars 2009.
   1.2 Finalisation du livrable. Cette action sera complétée en mai 2009.
   1.3 Validation du livrable. Cette action sera complétée en juillet 2009.
   1.4 Élaboration d'un plan de communication. Cette action sera complétée en mai 2009.
   1.5 Approbation finale par la Présidente-Directrice générale du Bureau de la traduction. Cette action sera complétée en août 2009.
   1.6 Exécution du plan de communication. Cette action sera complétée en août 2009.

2. Élaborer un processus pour régir la destruction des renseignements classifiés confiés au Bureau de la traduction et traités sur des systèmes appartenant à Travaux publics et Services gouvernementaux Canada..

   Réponse du Bureau de la traduction. Le Bureau de la traduction accepte la recommandation et prendra les mesures suivantes:

   Livrable : directive (processus et procédures).

   2.1 Identification des éléments manquants au cadre et procédures existants du Bureau de la traduction. Cette action sera complétée en mars 2009.
   2.2 Finalisation du livrable. Cette action sera complétée en mai 2009.
   2.3 Validation du livrable. Cette action sera complétée en juillet 2009.
   2.4 Élaboration d'un plan de communication. Cette action sera complétée en mai 2009.
   2.5 Approbation finale par la Présidente-Directrice générale du Bureau de la traduction. Cette action sera complétée en août 2009.
   2.6 Exécution du plan de communication. Cette action sera complétée en août 2009.

3. Certifier et accréditer les systèmes appartenant à Travaux publics et Services gouvernementaux Canada utilisés par le personnel du Bureau de traduction pour le soutien à la traduction de renseignements classifiés.

   Réponse du Bureau de la traduction. Le Bureau de la traduction accepte la recommandation et prendra les mesures suivantes :

   Livrable : Certification et accréditation des solutions technologiques-types de traitement des renseignements classifiés du Bureau de la traduction.

   3.1 Revue des actions à compléter dans le cadre du processus de certification en cours avec la Direction de la sécurité de la technologie de l'information. Cette action sera complétée en avril 2009.
   3.2 Compléter toutes les étapes du processus normalisé de certification et d'accréditation des solutions technologiques-types de traitement des renseignements classifiés du Bureau de la traduction;
      3.2.1 Confirmation du processus de certification et d'accréditation selon le niveau d'effort. Cette action sera complétée en avril 2009.
      3.2.2 Confirmation du plan de certification auprès de la Direction de la sécurité de la technologie de l'information. Cette action sera complétée en mai 2009.
      3.2.3 Énoncé des risques acceptables. Cette action sera complétée en juillet 2009.
      3.2.4 Validation de l'architecture/la conception auprès de la Direction de la sécurité de la technologie de l'information. Cette action sera complétée en octobre 2009.
      3.2.5 Validation des exigences de la sécurité auprès de la Direction de la sécurité de la technologie de l'information. Cette action sera complétée en février 2009.
      3.2.6 Rapport sur les éléments probants de la certification. Cette action sera complétée en avril 2010.
      3.2.7 Lettre de certification émise par l'autorité de certification des systèmes et applications du Bureau de la traduction, en l'occurrence le directeur, direction de la sécurité de la technologie de l'information du Bureau du DPI au sein de la direction générale des services d'infotechnologie. Cette action sera complétée en juin 2010.
   3.3 Approbation finale de la lettre d'accréditation par l'autorité d'accréditation des systèmes et applications du Bureau de la traduction, en l'occurrence la Présidente-Directrice générale du Bureau de la traduction. Cette action sera complétée en juin 2010.

Réponse de la direction

44. La Direction générale des ressources humaines considère que les résultats de la vérification reflètent de façon juste et exacte l'état du cadre de contrôle de la gestion visant à protéger le Système de gestion des ressources humaines contre l'accès non autorisé. La Direction générale des ressources humaines a l'intention d'agir suite aux recommandations de la vérification, en mettant en place le plan d'action de la gestion décrit plus-bas.

45. La sous-ministre adjointe de la Direction générale des ressources humaines devrait :

1. Répondre à toutes les recommandations en suspens relativement à la gestion des accès contenues dans l'évaluation de la menace et des risques datée du 2007-12-20.

   Réponse de la Direction générale des ressources humaines. La Direction générale des ressources humaines accepte la recommandation et prendra les mesures suivantes :

   1.1 Afin d'adresser la première recommandation de menace et des risques (Considérer le cryptage de transfert de données pour améliorer la sécurité), la direction générale des ressources humaines conclura un accord écrit avec la direction générale des services d'infotechnologie pour s'assurer que des données protégées de B transmises entre le système de gestion des ressources humaines et d'autres systèmes de TPSGC sont cryptées. Cette action sera complétée le 31 mars 2009.
   1.2 La direction générale des ressources humaines fera le suivi sur les progrès par rapport à l'accord jusqu'à ce que toutes les interfaces entre le système de gestion des ressources humaines et d'autres systèmes de TPSGC, et entre les deux composantes identifiées dans l'évaluation de la menace et des risques, soient modifiées pour s'assurer que les données protégées B transmises sont cryptées. Cette action sera complétée le 31 mars 2010
   1.3 À l'automne 2008, l'intention était de migrer à PeopleSoft, y compris toutes les données historiques du système de gestion des ressources humaines. Cependant, en raison du manque de fonds, le projet a été retardé et, la décision de ne pas migrer toutes les données historiques a été prise basée sur une approche plus efficace et moins onéreuse. Par conséquent, pour adresser la deuxième recommandation de l'évaluation de la menace et des risques liée à la gestion d'accès (considérer le déplacement vers un environnement protégé plus approprié), la direction générale des ressources humaines conclura un accord écrit avec la direction générale des services d'infotechnologie pour s'assurer que le système de gestion des ressources humaines est logé dans un environnement approprié contrôlé par la direction générale des services d'infotechnologie. Cette action sera complétée le 30 juin 2009.
   1.4 La direction générale des ressources humaines fera le suivi sur les progrès par rapport à l'accord jusqu'à ce que les travaux exigés, pour loger le système de

gestion des ressources humaines dans un environnement approprié, soient terminés. Cette action sera complétée le 31 mars 2011.

À PROPOS DE LA VÉRIFICATION

Autorisation

La vérification a été approuvée par le Comité de vérification et d'évaluation du ministère dans le cadre du Plan de vérification interne 2008-2009.

Objectifs

L'objectif de cette vérification interne était de déterminer si le cadre de contrôle de la gestion des accès en place était suffisant pour protéger contre l'accès non autorisé à certains systèmes d'infotechnologie déterminés.

Plus précisément, cette vérification a évalué si des mesures appropriées étaient en place afin de contrôler et limiter l'accès aux systèmes et aux renseignements sensibles, en limitant l'accès aux personnes qui détiennent une approbation officielle, la côte de sécurité requise et ont un accès sélectif.

Portée et approche

La présente vérification a été réalisée entre les mois de février et juillet 2008.

La portée de la vérification comprenait la gestion des accès aux systèmes utilisés dans deux points de service pour le soutien à la traduction de documents classifiés par le Bureau de la traduction; et le Système de gestion des ressources humaines (SGRH).

La sécurité physique des systèmes vérifiés ainsi que la sécurité de l'infrastructure de services partagés de TI n'ont pas été examinées.

Des membres clés du personnel ont été interviewés. Les processus et les documents pertinents ont fait l'objet d'une révision. En fonction de l'analyse de l'information et des preuves recueillies, l'équipe de vérification a formulé des observations et des conclusions par rapport à la vérification, qui ont été attestées par les gestionnaires compétents avant le dépôt de l'ébauche du rapport final auprès du Comité de vérification et d'évaluation de TPSGC.

La vérification a été réalisée conformément à la *Politique de vérification interne* du Conseil du Trésor et aux normes de vérification interne du gouvernement du Canada.

Critères

Les critères pour la réalisation de la présente vérification ont été élaborés à partir de la *Politique du gouvernement sur la sécurité (PGS)* et de la *Norme Gestion de la sécurité des technologies de l'information (GSTI).*

Les critères de vérification suivants ont été utilisés pour la présente vérification :

a) Le cadre de gestion sur le contrôle des accès est conforme à la Politique sur la sécurité du gouvernement, et des documents connexes (normes, directives, lignes directrices et procédures) ont été développés, diffusés et sont maintenus.

b) L'accès aux applications et aux systèmes de soutien, est accordé seulement aux personnes qui ont obtenu la côte de sécurité requise.

c) Un gestionnaire bien renseigné et responsable a accordé une autorisation officielle d'accès à la personne ayant besoin d'accéder à des renseignements ou à des biens de nature délicate, selon le principe du « privilège minimal ».

d) Des mesures d'identification et d'authentification des accès ont été intégrées aux applications et aux systèmes de soutien, en fonction du niveau de risque pour l'application ou pour le système.

e) Les privilèges d'accès sont mis à jour régulièrement pour correspondre exactement aux responsabilités actuelles de la personne; ils sont révisés lorsque ces personnes sont mutées à un poste qui ne requiert pas le même niveau d'accès et sont retirés aux personnes qui quittent l'organisation.

f) La séparation des responsabilités se reflète dans les privilèges d'accès; aucune personne ne détient le contrôle unique de tous les aspects d'un processus ou d'un système; les personnes autorisées à effectuer des opérations sensibles ne doivent pas être autorisées à en faire la vérification.

g) Des processus sont en place pour assurer que les accès non autorisés sont détectés, font l'objet d'une enquête, que des mesures sont prises pour minimiser les répercussions, et qu'une mesure administrative, corrective ou disciplinaire pertinente est prise.

Fin des travaux de vérification

Le travail de vérification sur le terrain a été effectivement achevé le 8 juillet 2008.

Équipe de vérification

La vérification a été réalisée par un membre du Bureau de la vérification et de l'évaluation et par un expert-conseil encadré par le directeur, Vérification de l'infotechnologie, sous la direction générale de la dirigeante principale de la vérification, Bureau de la vérification et de l'évaluation. Un expert-conseil additionnel sous la supervision du directeur, Vérification de l'infotechnologie, a contribué à la rédaction du rapport de vérification.

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