Commissariat
à la protection de la
vie privée du Canada

AGENCE DU REVENU DU CANADA

Rapport de vérification de la commissaire à la protection de la vie privée du Canada

Article 37 de la *Loi sur la protection des renseignements personnels*

RAPPORT FINAL

2013

Commissariat à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario)
K1A 1H3

613-947-1698, 1-800-282-1376
Téléc. : 613-947-6850
ATS : 613-992-9190
Suivez-nous sur Twitter : @PriveePrivacy

No de catalogue IP54-53/2013
ISBN 978-1-100-54620-9

Cette publication est également disponible sur notre site Web à **www.priv.gc.ca**.

Table des matières

Principaux éléments

POINTS EXAMINÉS

L'Agence du revenu du Canada (l'ARC ou l'Agence) applique les lois fiscales et administre divers programmes de prestations au nom du gouvernement du Canada et de plusieurs provinces et territoires. Pour ce faire, elle doit recueillir et utiliser des renseignements sur les contribuables. Nous nous sommes penchés sur la façon dont l'Agence gère ces renseignements, et plus particulièrement sur les procédures relatives à l'octroi et à la surveillance des droits d'accès à ces derniers.

Au cours de notre vérification, qui a eu lieu du 13 juillet 2012 au 31 mars 2013, nous avons examiné la façon dont l'Agence assigne les responsabilités liées à la protection des renseignements personnels, gère les risques d'atteinte à la vie privée et veille au respect de la *Loi sur la protection des renseignements personnels*. Nous avons passé en revue les politiques et les procédures en matière de gestion des renseignements personnels, les documents de formation, les évaluations des facteurs relatifs à la vie privée, les enquêtes sur les atteintes à la vie privée, les vérifications internes et les examens de la sécurité de l'Agence. Nous nous sommes aussi penchés sur la sécurité des technologies de l'information, l'accès aux systèmes électroniques et la surveillance des employés qui accèdent quotidiennement à des renseignements sur les contribuables. Enfin, nous avons interviewé de nombreux employés de l'Agence qui travaillent à l'administration centrale et dans les quatre plus grands bureaux régionaux, soit ceux de l'Ontario, du Pacifique, des Prairies et du Québec.

IMPORTANCE DE CET ENJEU

L'Agence, qui perçoit l'impôt sur le revenu et verse des prestations à plus de 27 millions de contribuables canadiens, dispose de l'une des plus importantes banques de renseignements personnels au Canada.

Les dossiers des contribuables renferment en outre des renseignements de nature très délicate permettant de les identifier et portant sur leur état de santé et leur situation financière, professionnelle et familiale.

Les renseignements sur les contribuables constituent la pierre angulaire de l'administration des programmes et des services liés à l'impôt de l'ARC. L'Agence a besoin des renseignements personnels des Canadiens pour percevoir l'impôt nécessaire au financement des programmes et des services publics.

L'ARC exerce ses activités de perception des impôts à l'intérieur du cadre d'un régime d'observation volontaire. L'an dernier, plus de 91 % des Canadiens ont rempli une déclaration de revenus, et 94 % ont payé le montant dû dans les délais prescrits. Par ailleurs, les contribuables s'attendent à ce que l'Agence et ses employés fassent preuve de vigilance et prennent toutes les mesures nécessaires pour empêcher la consultation, l'utilisation ou la communication inappropriée de leurs renseignements personnels.

Au cours des dernières années, le Commissariat a été avisé d'atteintes à la vie privée à l'Agence résultant de l'accès inapproprié à des renseignements sur les contribuables. Ce sont des employés, des plaignants ou les médias qui l'ont mis au courant.

Les atteintes à la vie privée pourraient avoir de graves conséquences sur les personnes touchées (fraude ou vol d'identité, difficultés financières ou embarras personnel), en plus de ternir la réputation de l'Agence à titre de gardienne de confiance des renseignements personnels de nature délicate des Canadiens.

CONSTATATIONS

Il règne, à l'ARC, une culture de sécurité et de confidentialité qui est attribuable à la présence d'un cadre d'intégrité, de politiques, d'activités de formation et de sensibilisation, ainsi que d'autres initiatives. On décèle toutefois des lacunes prononcées sur le plan de la mise en œuvre et de la surveillance de certaines de ses principales politiques et pratiques en matière de sécurité et de protection de la vie privée. Ces lacunes nuisent à la capacité de l'ARC de protéger pleinement les renseignements sur les contribuables contre toute consultation, utilisation ou communication inappropriée. Plus particulièrement, on constate :

- qu'afin de respecter une recommandation formulée lors de la vérification de 2009, un chef de la protection des renseignements personnels (CPRP) a été nommé le 3 avril 2013. Le rôle du CPRP n'a cependant pas encore été défini avec précision aux fins de la coordination des obligations relatives à la reddition de comptes, aux responsabilités et aux activités liées à la protection de la vie privée à l'échelle de l'Agence;
- que des évaluations des facteurs relatifs à la vie privée ne sont pas toujours réalisées afin d'évaluer les risques associés à des changements relatifs aux programmes qui auront des répercussions sur les renseignements personnels des contribuables;
- que de nombreux systèmes informatiques qui traitent des renseignements sur les contribuables ne font pas l'objet d'une évaluation de la menace et des risques, ce qui pourrait faire en sorte que des lacunes ne soient pas décelées;
- que l'efficacité des contrôles mis en œuvre par l'Agence afin de repérer et de prévenir toute consultation ou utilisation inappropriée de renseignements sur les contribuables par des employés est limitée par l'absence d'un outil automatisé permettant de repérer et de signaler les potentiels cas d'accès inapproprié ainsi que par certaines lacunes au chapitre de la collecte de données permettant d'établir une piste de vérification dans les systèmes informatiques de l'ARC;
- que des cas d'accès inapproprié aux dossiers de milliers de contribuables sont passés inaperçus pendant une longue période;
- que la Direction de l'accès à l'information et de la protection des renseignements personnels n'est pas régulièrement informée des atteintes à la vie privée résultant de la consultation et de la communication inappropriée de renseignements sur les contribuables.

Depuis la parution du rapport portant sur la dernière vérification effectuée par le Commissariat, en 2009, l'ARC a effectué des progrès en ce qui a trait au renforcement de ses politiques et de ses procédures en matière de sécurité et de protection de la vie privée, ainsi qu'en ce qui concerne la communication de ses attentes à l'égard de la protection des renseignements personnels à ses employés. L'Agence déploie également des efforts en vue d'améliorer la gestion des droits d'accès et de surveiller plus étroitement l'accès des employés aux renseignements sur les contribuables.

Les observations et les recommandations formulées dans le présent rapport ont pour but d'améliorer les pratiques de traitement des renseignements personnels de l'Agence et, ainsi, d'atténuer les risques de consultation, d'utilisation ou de communication non autorisée des renseignements personnels des contribuables.

L'Agence a répondu à nos conclusions. Chacune des recommandations formulées dans le rapport de vérification est suivie de la réponse de la direction de l'Agence.

Introduction

À PROPOS DE L'AGENCE DU REVENU DU CANADA

L'ARC applique les lois fiscales et administre divers programmes de prestations socioéconomiques et programmes d'encouragement au nom du gouvernement du Canada et de la plupart des provinces et des territoires.

Le ministre du Revenu national doit rendre compte au Parlement de toutes les activités de l'Agence, y compris de l'administration et de l'application de la *Loi de l'impôt sur le revenu*. Le Conseil de direction de l'ARC exerce un rôle de surveillance de l'organisation au nom du ministre et est responsable de la planification stratégique de celle-ci.

Le commissaire de l'Agence qui est nommé au poste de premier dirigeant de l'ARC est responsable des activités quotidiennes liées à l'administration et au respect des diverses lois, dont la *Loi de l'impôt sur le revenu* et la *Loi sur la protection des renseignements personnels*. Le commissaire et les sous-commissaires siègent au Comité de direction de l'Agence, qui fournit une orientation stratégique, contrôle la gestion et assume les responsabilités liées à la gestion du risque pour l'ensemble de l'organisation.

Pour s'acquitter de son mandat de percepteur des impôts au Canada, l'ARC dispose de l'une des plus importantes banques de renseignements personnels au Canada. En 2012, l'Agence a reçu près de 27 millions de déclarations de revenus des particuliers, versé plus de 34 millions de paiements d'impôts, accordé 111 millions de crédits d'impôt et de prestations à quelque 12 millions de Canadiens et répondu à près de 18 millions de demandes de renseignements de la part du public. De toutes les organisations gouvernementales, l'ARC est celle qui interagit avec le plus grand nombre de Canadiens, et ses activités ont des répercussions importantes sur les particuliers et les entreprises.

En 2012, l'ARC comptait environ 40 000 employés répartis dans cinq bureaux régionaux et dans quarante centres et points de services fiscaux partout au Canada. Approximativement 65 pour cent (soit 26 000) de ces employés peuvent accéder électroniquement à des renseignements sur les contribuables au moyen de différents systèmes informatiques aux fins de l'impôt.

L'ARC est assujettie à la *Loi sur la protection des renseignements personnels* et aux politiques et directives connexes du Conseil du Trésor concernant la gestion et la protection des renseignements personnels des Canadiens. L'article 241 de la *Loi de l'impôt sur le revenu* énonce aussi les exigences en matière de confidentialité que les employés et toute autre personne ayant accès aux renseignements sur les contribuables doivent respecter. Des pénalités peuvent être imposées si la *Loi* n'est pas respectée.

Encadré 1 : Protection des renseignements sur les contribuables en vertu de la *Loi de l'impôt sur le revenu*

241. (1) Sauf autorisation prévue au présent article, il est interdit à un fonctionnaire ou autre représentant d'une entité gouvernementale :

a) de fournir sciemment à quiconque un renseignement confidentiel ou d'en permettre sciemment la prestation;

b) de permettre sciemment à quiconque d'avoir accès à un renseignement confidentiel;

c) d'utiliser sciemment un renseignement confidentiel en dehors du cadre de l'application ou de l'exécution de la présente loi, du Régime de pensions du Canada, de la *Loi sur l'assurance-chômage* ou de la *Loi sur l'assurance-emploi*, ou à une autre fin que celle pour laquelle il a été fourni en application du présent article.

De plus amples renseignements au sujet de l'Agence sont disponibles à l'adresse www.cra-arc.gc.ca.

CENTRE D'INTÉRÊT DE LA VÉRIFICATION

La vérification était axée sur l'accès électronique des employés aux renseignements sur les contribuables. Elle visait à déterminer si l'ARC avait mis en place les contrôles et les mesures nécessaires pour protéger les renseignements personnels des contribuables et si ses politiques, processus, procédures et pratiques étaient conformes aux principes relatifs à l'équité dans le traitement de l'information qui sont énoncés aux articles 4 à 8 de la *Loi sur la protection des renseignements personnels*.

La vérification ne comprenait pas un examen des pratiques de gestion des renseignements personnels liés à l'imposition des clients commerciaux, à la taxe sur les produits et services, à la taxe de vente harmonisée ou aux opérations liées à la taxe d'accise. Elle ne portait pas non plus sur des aspects comme l'accès de tiers aux renseignements concernant des contribuables donnés, l'accès des contribuables aux services de l'Agence par Internet et le récent transfert de certains services de TI à Services partagés Canada.

Observations et recommandations

1. Les observations et recommandations découlant de la vérification sont regroupées en quatre catégories :
   - la gestion de la protection de la vie privée et la responsabilité à cet égard;
   - la sécurité et gouvernance des technologies de l'information;
   - le contrôle de l'accès des employés;
   - les atteintes à la vie privée.

GESTION DE LA PROTECTION DE LA VIE PRIVÉE ET RESPONSABILITÉ À CET ÉGARD

2. La *Loi sur la protection des renseignements personnels* oblige les organisations à établir des mécanismes de reddition de comptes visant à assurer le respect de celle-ci. Nos vérifications antérieures d'institutions gouvernementales ont démontré qu'en l'absence de mécanismes de reddition de comptes clairement définis, on recense des lacunes sur le plan de la coordination et de la mise en œuvre des responsabilités en matière de protection de la vie privée. Ces lacunes au chapitre de la reddition de comptes peuvent mettre en risque la confidentialité des renseignements personnels.

3. Le ministre du Revenu national est responsable de l'application de la *Loi sur la protection des renseignements personnels* et du respect des instruments de politique du Conseil du Trésor à l'ARC. À titre de premier dirigeant de l'Agence, le commissaire veille à l'application quotidienne de la législation relative aux programmes qui relève des pouvoirs délégués par le ministre et au respect global de la *Loi sur la protection des renseignements personnels*.

4. Le directeur de l'accès à l'information et de la protection des renseignements personnels (AIPRP) est responsable en grande partie de l'exécution du programme de protection de la vie privée à multiples volets de l'Agence. La Direction de l'AIPRP traite les demandes et les plaintes relatives à la protection des renseignements personnels, élabore des politiques, des procédures et des documents de formation, examine les évaluations des facteurs relatifs à la vie privée et formule des recommandations à cet égard, et analyse les atteintes à la vie privée. Le directeur préside aussi le Comité d'examen de surveillance de l'AIPRP, qui permet aux directeurs d'aborder et de régler les questions liées à l'accès à l'information et à la protection des renseignements personnels. Le directeur relève du sous-commissaire, Affaires publiques, qui siège au Comité de direction de l'Agence.

5. Au cours des dernières années, l'ARC a élaboré une série exhaustive de politiques et de documents connexes en matière de protection de la vie privée, dont une politique sur la protection des renseignements personnels, une directive sur les pratiques relatives à la protection de la vie privée, des procédures pour la réalisation des évaluations des facteurs relatifs à la vie privée, un protocole en cas d'atteinte à la vie privée et une politique sur l'imposition de sanctions disciplinaires. Dans l'ensemble, le cadre de gestion et de reddition de comptes en matière de protection de la vie privée de l'Agence comporte plusieurs éléments utiles pour assurer la protection des renseignements personnels des contribuables.

La responsabilité pour la protection des renseignements personnels doit être définie

6. Compte tenu du grand nombre de renseignements sur les contribuables détenus par l'Agence et de la nature très délicate de ces renseignements, nous nous attendions à constater que l'ARC avait nommé un chef de la protection des renseignements personnels et lui avait confié des pouvoirs considérables afin qu'il puisse améliorer et surveiller le programme de protection de la vie privée de l'Agence et veiller au respect de la *Loi sur la protection des renseignements personnels*.

7. De nombreuses organisations des secteurs public et privé ont compris qu'il fallait absolument charger un cadre supérieur de veiller à la protection des renseignements personnels des clients pour préserver la confiance et la bonne volonté de ces derniers. La confiance des clients est aussi essentielle pour permettre à une organisation de s'acquitter de son mandat, et d'exécuter ses programmes et de fournir ses services de manière efficace et efficiente.

8. La *Loi sur la protection des renseignements personnels* n'oblige pas les institutions fédérales à nommer un chef de la protection des renseignements personnels, et les politiques du Conseil du Trésor ne définissent pas le rôle de ce dernier[1]. Néanmoins, la désignation d'un chef de la protection des renseignements personnels est une pratique de plus en plus répandue chez les grandes organisations qui sont responsables de gérer un volume important de renseignements personnels de nature délicate. Le chef de la protection des renseignements personnels, qui est issu des rangs de la haute direction de l'organisation, est responsable de la direction stratégique globale du dossier de la protection de la vie privée et de veiller au respect de la loi par l'organisation.

9. Le chef de la protection des renseignements personnels est également responsable de veiller à ce que les nouveaux programmes dans le cadre desquels des renseignements personnels sont traités fassent l'objet d'évaluations des facteurs relatifs à la vie privée. Comme ces rôles se chevauchent, le chef de la protection des renseignements personnels est habituellement membre du Comité de la haute direction de l'organisation, ce qui lui permet d'entretenir ses collègues des questions liées à la protection des renseignements personnels avec autorité, de s'assurer que les enjeux sont bien compris et de demander à la direction d'appuyer des mesures visant à réduire les risques d'atteinte à la vie privée à l'échelle de l'organisation.

10. À la suite de la vérification des cadres de gestion de la protection de la vie privée que nous avons effectuée en 2009, nous avons recommandé que l'ARC nomme un chef de la protection des renseignements personnels, ce qu'elle a accepté de faire. L'ARC a élaboré un cadre provisoire pour la nomination d'un tel chef, mais ce cadre n'a pas été mis en œuvre et aucun chef de la protection des renseignements personnels n'a été nommé. Par conséquent, jusqu'à tout récemment, l'Agence ne pouvait pas compter sur un champion de la protection des renseignements personnels parmi ses cadres supérieurs pour promouvoir le respect de la vie privée à l'échelle de l'organisation. Cela dit, depuis 2009, le personnel de l'AIPRP a élaboré un certain nombre de politiques et de procédures importantes liées à la protection de la vie privée et a mis sur pied diverses initiatives de formation.

11. Le 3 avril 2013, le commissaire du Revenu a informé le personnel de l'Agence qu'un sous-commissaire avait été nommé chef de la protection des renseignements personnels afin d'assurer le respect de la *Loi sur la protection des renseignements personnels* et d'assumer

[1] Le Commissariat a publié un guide pour aider les organisations à définir le rôle du chef de la protection des renseignements personnels en fonction de leurs besoins particuliers (*Un programme de gestion de la protection de la vie privée : la clé de la responsabilité*, 2012). Bien que ce document vise les organisations assujetties à la législation en matière de protection des renseignements personnels qui s'applique au secteur privé, les institutions du secteur public pourraient le trouver utile.

d'autres rôles sur les plans de la gestion, de la sensibilisation, de l'évaluation des risques et de la reddition de comptes. Cette nomination constitue un grand pas en vue du renforcement du régime de gestion de la protection de la vie privée de l'Agence. Toutefois, afin que le plein effet d'une telle nomination se fasse sentir à l'échelle de l'organisation, le mandat, le rôle et les principales activité du chef de la protection des renseignements personnels doivent être officialisés et définis avec plus de précision.

12. RECOMMANDATION

L'Agence du revenu du Canada devrait définir avec précision le rôle du chef de la protection des renseignements personnels et surveiller la mise en œuvre de son mandat en ce qui a trait à la sensibilisation des employés à la protection des renseignements personnels, à la réduction du risque d'atteinte à la vie privée et au respect global de la *Loi sur la protection des renseignements personnels* par l'Agence.

Réponse de l'Agence :

Comme le souligne le rapport, la Loi sur la protection des renseignements personnels *n'oblige pas les institutions fédérales à nommer un chef de la protection des renseignements personnels, et les politiques du Conseil du Trésor ne définissent pas le rôle de ce dernier.*

Néanmoins, l'Agence du revenu du Canada (ARC) est d'accord avec la recommandation et a nommé un chef de la protection des renseignements personnels qui est chargé de la surveillance de la gestion de la protection de la vie privée à l'Agence en avril 2013. Le chef de la protection des renseignements personnels fait partie du Comité de direction de l'Agence et s'est vu confier le vaste mandat d'assurer la protection de la vie privée à l'Agence, notamment :

- *en exerçant un droit de regard sur les décisions relatives à la protection des renseignements personnels, y compris les évaluations des facteurs relatifs à la vie privée;*
- *en défendant le droit à la vie privée des particuliers conformément aux lois et aux politiques en vigueur, ce qui comprend la gestion des cas d'atteinte à la vie privée au sein de l'Agence — une responsabilité qu'il partage avec l'équipe de la Sécurité;*
- *en supervisant la sensibilisation au respect de la vie privée à l'Agence au moyen de la mise sur pied de diverses activités de communication et de formation.*

Le chef de la protection des renseignements personnels, qui assure la liaison avec le Commissariat à la protection de la vie privée, surveillera le respect global de la Loi sur la protection des renseignements personnels *par l'Agence et fera rapport à la haute direction de la situation au chapitre de la gestion de la protection de la vie privée au sein de l'organisation au moins deux fois par année financière.*

Les employés comprennent leur devoir en ce qui a trait à la protection des renseignements sur les contribuables

13. Le respect des exigences et de l'esprit de la *Loi sur la protection des renseignements personnels* dépend en grande partie de la compréhension qu'a le personnel qui traite des renseignements personnels de ses obligations en vertu de cette loi. Les employés doivent être informés des politiques, des procédures et des lignes directrices de l'organisation en ce qui a trait à la protection de la vie privée et devraient bien comprendre leurs rôles et leurs responsabilités à l'égard de la protection des renseignements personnels des clients.

14. Nous nous attendions donc à constater que l'ARC avait mis en place des mesures concernant la formation et la sensibilisation afin de garantir que ses employés comprennent pleinement leurs responsabilités à l'égard de la gestion et de la protection adéquates des renseignements sur les contribuables. Nous avons examiné les documents de formation en matière de protection de la vie privée, de sécurité, et de valeurs et d'éthique, ainsi que d'autres ressources documentaires à la disposition des employés sur le site intranet de l'Agence. Nous avons aussi interviewé des employés et reçu

de l'information des personnes chargées de la coordination des initiatives de formation en matière de protection de la vie privée et de sécurité.

15. Pour l'Agence, qui compte près de 26 000 employés qui accèdent quotidiennement aux renseignements sur les contribuables, offrir une formation continue en matière de protection de la vie privée et de sécurité de l'information représente une tâche colossale; c'est pourquoi l'ARC recourt à des mécanismes tant formels qu'informels pour sensibiliser ses employés.

16. Nous avons constaté que l'ARC a consacré beaucoup de temps et des ressources considérables à l'élaboration de plans de formation exhaustifs en matière de protection de la vie privée et de sécurité de l'information. La formation sur la protection de la vie privée comprend des séances en personne et d'autres activités de sensibilisation offertes sur le site intranet de l'Agence, par courriel ou dans le cadre de rencontres avec les employés. Plus de 5 600 employés et gestionnaires de l'ARC ont reçu une formation directe en matière de protection de la vie privée depuis 2010. L'Agence continue de déployer des efforts considérables pour maintenir et accroître la sensibilisation à la protection de la vie privée.

17. Les entrevues réalisées avec les gestionnaires et les superviseurs de l'ARC ont permis de confirmer que ces derniers avaient reçu une formation sur la protection de la vie privée et la sécurité de l'information. Ces gestionnaires de niveau intermédiaire supervisent un grand nombre d'employés de première ligne. Nous avons aussi constaté qu'ils comprenaient bien leur obligation de veiller à ce qu'eux-mêmes et leurs subalternes respectent et protègent les renseignements personnels en tout temps.

Des outils ont été conçus pour évaluer les risques d'atteinte à la vie privée

18. Selon le Cadre stratégique de gestion du risque du Conseil du Trésor, il incombe aux administrateurs généraux de gérer les risques de leur organisation en dirigeant la mise en œuvre de pratiques efficaces de gestion du risque, tant officielles que non officielles.

19. Les organisations se servent d'un éventail d'outils pour évaluer et gérer les risques d'atteinte à la vie privée, y compris des évaluations des risques organisationnels, des vérifications internes, des évaluations de la menace et des risques et des évaluations des facteurs relatifs à la vie privée. Nous nous attendions à ce que l'Agence utilise, selon les circonstances, un ou plusieurs des outils susmentionnés pour évaluer, limiter et atténuer les risques liés à la gestion et à la protection des renseignements sur les contribuables.

20. La politique de gestion des risques de l'ARC exige l'élaboration d'un plan de gestion des risques pour l'organisation afin d'évaluer et de rendre compte d'une série de risques importants pour l'ensemble de l'Agence sur le plan des opérations et du respect de la loi. En matière de gestion des risques organisationnels, l'Agence adopte une approche « tous risques », ce qui signifie qu'elle prend en considération tant les risques inhérents que les risques actuels.

21. Un sous-commissaire assume les fonctions d'agent principal de la gestion des risques à l'ARC et dirige le processus de planification des risques de l'Agence. Récemment, cette même personne a accepté d'exercer les fonctions complémentaires de dirigeant principal de la vérification.

22. Le processus de planification des risques de l'Agence prévoit un examen triennal des risques ayant une incidence sur le mandat de l'organisation. Cet examen regroupe les évaluations des risques réalisées par plusieurs grands secteurs de programme et les combine pour former une évaluation des risques organisationnels et un plan d'action pour l'ensemble de l'Agence. Des études annuelles des risques organisationnels sont aussi menées afin d'intégrer les nouveaux enjeux au plan.

23. Le profil de risque organisationnel établit un lien important entre les risques liés à la protection des renseignements et ceux qui sont associés au comportement éthique des employés. Il indique aussi que les risques appartenant à ces deux catégories pourraient avoir une incidence directe sur la réputation et l'image publique de l'Agence. Si un employé de l'Agence venait à utiliser de façon inappropriée les renseignements personnels

de contribuables et que l'incident était rendu public, il ne fait aucun doute que la confiance des Canadiens en l'Agence risquerait d'être ébranlée.

24. L'ARC a aussi procédé à des vérifications internes et à d'autres examens afin d'évaluer la gestion des droits d'accès des employés et de surveiller l'utilisation que font les employés des renseignements personnels. Ces vérifications et études ont aidé l'Agence à brosser un tableau de la situation actuelle en ce qui a trait à l'accès des employés. Grâce à ces activités de vérification interne, l'ARC a pu cerner les lacunes dans ses contrôles et concevoir une stratégie à long terme pour la mise en œuvre de nouvelles mesures et l'amélioration des mesures existantes dans le but de réduire les risques en matière de sécurité et de protection de la vie privée.

Une évaluation des facteurs relatifs à la vie privée ne précède pas toujours la mise en œuvre d'un projet

25. L'évaluation des facteurs relatifs à la vie privée (EFVP) est un outil qui permet d'évaluer les risques en matière de vie privée découlant de la mise en œuvre d'un projet, d'une initiative ou d'un programme, ou encore de l'apport de changements à un projet, une initiative ou un programme qui existe déjà. L'EFVP prédit les conséquences et les torts probables que les risques cernés pourraient entraîner en ce qui a trait à la confidentialité des renseignements personnels des clients et à la réputation de l'organisation. Enfin, les organisations peuvent se servir de l'EFVP de façon proactive pour mettre au point des solutions visant à prévenir ou à limiter les risques en matière de vie privée liés aux renseignements personnels des clients.

26. L'EFVP est conçue pour fournir une précieuse analyse des risques en matière de vie privée dès les premières étapes du processus de planification de projet. Réaliser une EFVP avant de mettre en œuvre un programme ou un service permet d'éviter, du moins en partie, les complications ou les coûts qui pourraient découler de la modification, du report ou de l'annulation dudit programme ou service dans le cas où des risques en matière de vie privée seraient cernés après la mise en œuvre de ce dernier. En règle générale, il est beaucoup plus rentable et efficace de prévoir des mesures de protection de la vie privée dès le début d'un projet plutôt que d'essayer de les intégrer par la suite.

27. Le Conseil du Trésor a instauré une politique concernant les EFVP en 2002 afin de garantir la prise en considération des principes et des mesures de protection de la vie privée dans le cadre de tous les nouveaux programmes et services (ou des programmes et des services ayant été remaniés en profondeur) du secteur public fédéral. Cette politique a été remplacée par la Directive sur l'évaluation des facteurs relatifs à la vie privée en avril 2010. Pour se conformer à la Directive, une organisation doit mettre en place des mécanismes permettant de cerner et d'examiner toute activité nouvelle ou remaniée ayant une incidence sur la gestion des renseignements personnels. Afin de déterminer si une évaluation officielle des risques en matière de vie privée s'impose, les organisations procèdent d'abord généralement à une évaluation préliminaire des risques en matière de vie privée qui pourraient découler de la mise en œuvre d'un nouveau programme ou du remaniement d'un programme existant.

Encadré 2 : Quand une EFVP s'impose-t-elle?

En règle générale, une EFVP s'impose si un programme nouveau ou remanié :

- utilise ou utilisera des renseignements personnels dans le cadre d'un processus décisionnel touchant directement un individu;
- modifie substantiellement des activités ou des programmes existants dans le cadre desquels des renseignements personnels sont utilisés, ou sont destinés à être utilisés, dans le cadre d'un processus décisionnel touchant directement un individu;
- confie à un sous-traitant ou transfère l'exécution d'un programme ou d'un service à un autre ordre de gouvernement ou au secteur privé, entraînant ainsi des modifications importantes au programme ou à l'activité;
- remanie en profondeur un système ou un processus utilisé pour dispenser un programme au public;
- recueille des renseignements personnels qui ne seront pas utilisés dans le cadre d'un processus de décision touchant directement un individu, mais qui auront une incidence sur la protection de la vie privée.

Les ministères et organismes gouvernementaux réalisent leurs propres EFVP. L'équipe responsable des EFVP au sein d'une organisation regroupe souvent des spécialistes de divers secteurs, dont ceux des programmes, de la protection des renseignements personnels et de l'accès à l'information, des services juridiques et des technologies de l'information. Une fois revue et approuvée par l'organisation qui l'a réalisée, chaque EFVP est envoyée au Secrétariat du Conseil du Trésor, et une copie est transmise au Commissariat à la protection de la vie privée pour examen.

Source : Inspiré de la Directive sur l'évaluation des facteurs relatifs à la vie privée du Conseil du Trésor, avril 2010.

28. Compte tenu de ce qui précède, nous nous attendions à ce que l'ARC ait mis en place un cadre pour l'évaluation des risques en matière de vie privée associés aux programmes ou systèmes nouveaux ou ayant été remaniés en profondeur. Nous nous attendions aussi à constater que des EFVP étaient réalisées avant la mise en œuvre de tout programme ou projet nouveau ou remanié.

29. En 2012, l'ARC a mis en place des procédures et des modèles détaillés pour la réalisation des EFVP. Ces instructions précisent les rôles et les responsabilités dans le cadre du processus et offrent une approche étape par étape de la préparation, de l'examen et de l'approbation des EFVP. L'Agence a aussi rédigé un questionnaire concernant les EFVP qui permet au secteur de programme concerné et à la Direction de l'AIPRP de se renseigner sur les risques possibles en matière de vie privée et de déterminer si une EFVP s'impose.

30. Cinq dossiers de projets pour lesquels une EFVP devait être réalisée ont été choisis pour faire l'objet d'un examen à partir d'une liste compilée par l'Agence pour 2012. Tous les dossiers se trouvaient à l'étape de la préparation, de l'examen ou de l'approbation. Or, notre examen nous a permis de constater que bien que deux ans ou plus se soient écoulés depuis la mise en œuvre des projets, les EFVP requises n'avaient pas été réalisées. Les dossiers n'indiquaient pas non plus la date à laquelle une EFVP serait réalisée, le cas échéant.

31. Si les risques en matière de vie privée ne font pas l'objet d'une évaluation adéquate avant la mise en œuvre de programmes nouveaux ou remaniés, l'Agence pourrait être incapable d'établir leur incidence possible sur les contribuables et de trouver des solutions pour prévenir les risques et minimiser les dommages. En outre, dans de telles circonstances, il s'avère impossible pour le Commissariat de jouer son rôle dans le processus d'EFVP qui, aux termes de la Directive sur l'EFVP, consiste à étudier et à analyser tout programme ou projet nouveau ou remanié ainsi qu'à formuler des conseils.

32. RECOMMANDATION

Conformément à la Directive du Conseil du Trésor sur les évaluations des facteurs relatifs à la vie privée, l'Agence du revenu du Canada devrait réaliser, examiner et approuver une évaluation des facteurs relatifs à la vie privée avant la mise en œuvre de tout nouveau programme ou initiative susceptible de mettre en péril la confidentialité des renseignements sur les contribuables.

Réponse de l'Agence :

L'ARC est d'accord avec la recommandation et veillera à ce qu'une évaluation des facteurs relatifs à la vie privée soit réalisée, examinée et approuvée avant la mise en œuvre de tout nouveau programme ou initiative susceptible de mettre en péril la confidentialité des renseignements sur les contribuables.

Pour s'acquitter de cette obligation, le chef de la protection des renseignements personnels s'est vu confier la responsabilité globale de surveiller l'état d'avancement des EFVP, conformément à son mandat. Il vérifiera aussi régulièrement que les cadres supérieurs de l'organisation s'acquittent de leur responsabilité à l'égard de la réalisation d'EFVP et en fera rapport au commissaire et à la haute direction.

SÉCURITÉ ET GOUVERNANCE DES TECHNOLOGIES DE L'INFORMATION

33. La sécurité de l'information est pleinement assurée lorsqu'elle est appuyée par tous les paliers d'une organisation, qu'elle fait partie intégrante de la planification stratégique et opérationnelle et qu'elle est intégrée aux pratiques, à la culture et aux activités quotidiennes de l'organisation, ainsi qu'au comportement des employés.

34. De saines pratiques en matière de sécurité de l'information sont essentielles au respect des exigences de la *Loi sur la protection des renseignements personnels* qui sont liées à la protection des renseignements personnels des Canadiens. Les organisations doivent instaurer des contrôles appropriés pour garantir que les renseignements personnels ne sont pas consultés, utilisés, communiqués, modifiés ou détruits sans autorisation.

35. La Politique sur la sécurité du gouvernement du Conseil du Trésor énonce les exigences de base obligatoires en matière de sécurité que doivent respecter les organisations fédérales afin de protéger et de préserver la confidentialité et l'intégrité des actifs gouvernementaux, dont les renseignements personnels. La Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI) du Conseil du Trésor et d'autres politiques et normes en matière de sécurité établissent l'ensemble de règles que doivent suivre les organisations pour assurer la protection de leurs employés et de leurs actifs — y compris les renseignements personnels.

Les responsabilités en matière de sécurité des TI sont claires

36. La Politique sur la sécurité du gouvernement stipule que les ministères et organismes fédéraux doivent réaliser des évaluations des risques afin de déterminer s'ils doivent mettre en œuvre des mesures allant au-delà des exigences de base obligatoires pour protéger leurs actifs.

37. En novembre 2011, l'ARC a transféré certaines fonctions liées à l'infrastructure des TI à Services partagés Canada (SPC). Malgré ce transfert, l'Agence demeure responsable de garantir la protection des fonds de renseignements personnels en lien avec son infrastructure des TI.

38. Nous nous attendions à constater que l'ARC avait mis en place un solide cadre de gouvernance de la sécurité des TI, et que les obligations et responsabilités en découlant avaient été clairement communiquées aux employés, qui les avaient bien comprises. Nous avons passé en revue les politiques, les plans, les rapports, les documents liés aux projets et les mandats et procès-verbaux des comités; nous avons aussi réalisé des entrevues avec la direction et des employés de l'Agence.

39. De façon générale, le responsable de la sécurité à l'ARC est responsable de tous les volets de la sécurité à l'Agence, y compris de la sécurité des renseignements sur les contribuables. Un plan de sécurité conçu pour l'Agence énonce les principaux risques en matière de sécurité, de même que les stratégies et les plans visant à les atténuer. Ces documents sur la sécurité sont harmonisés avec le processus global de gestion des risques organisationnels, qui prévoit l'identification, la gestion et la protection des renseignements personnels et des autres actifs liés aux technologies de l'information.

40. L'Agence a mis sur pied un comité au niveau de la direction qui est composé de représentants des intervenants concernés et qui est chargé de superviser tous les volets de la sécurité à l'Agence, y compris la sécurité des renseignements. Un comité mixte de la haute direction se réunit en outre régulièrement pour passer en revue les initiatives en matière de sécurité stratégique et opérationnelle et formuler des conseils à leur sujet.

De nombreux systèmes ne font pas l'objet d'une évaluation de la menaces et des risques

41. La Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI) du Conseil du Trésor oblige les ministères et organismes fédéraux à faire certifier et accréditer leurs applications et leurs systèmes de TI avant d'approuver leur mise en œuvre, faute de quoi ils risquent d'exploiter un système ne répondant pas aux normes de sécurité du gouvernement et mettant involontairement en péril la confidentialité des renseignements personnels qu'il contient.

42. La certification vise à vérifier que les exigences en matière de sécurité établies pour un système ou un service de TI donné sont respectées et que les contrôles et mesures de sécurité fonctionnent comme prévu. L'accréditation signifie que la direction a autorisé l'exploitation du système ou service et a accepté le risque résiduel en s'appuyant sur la preuve de la certification.

43. Selon la Norme, une évaluation de la menace et des risques permet d'établir les exigences en matière de sécurité. Les organisations doivent appliquer des mesures de sécurité allant au-delà des exigences de base lorsqu'une évaluation de la menace et des risques le justifie.

44. La politique d'évaluation de la menace et des risques liés aux technologies de l'information de l'ARC stipule que tous les nouveaux systèmes et applications réseau devraient faire l'objet d'une telle évaluation à l'étape de la conception. Nous nous attendions à constater que l'infrastructure des TI de l'Agence faisait régulièrement et de façon continue l'objet d'une évaluation des risques en matière de sécurité dans le but de cerner et d'atténuer les menaces et les vulnérabilités.

45. Toutes les plateformes du système de l'ARC font actuellement l'objet d'une évaluation dans le cadre d'un processus harmonisé d'évaluation de la menace et des risques. Toutefois, l'Agence a recensé un grand nombre d'applications traitant les renseignements des contribuables pour lesquelles une évaluation de la sécurité adéquate n'a pas été réalisée et pour lesquelles les processus relatifs à l'évaluation de la menace et des risques ainsi qu'à la certification et à l'accréditation n'ont pas été menés à bien.

46. Nous avons constaté que l'Agence mettait à l'essai un processus de certification et d'accréditation[2] qui prévoit l'utilisation d'un instrument de suivi et de vérification afin d'assurer la mise en œuvre des mesures recommandées à la suite des évaluations des risques. Cependant, l'examen des principaux documents relatifs à la certification et à l'accréditation de divers projets a révélé qu'un suivi n'était pas toujours effectué pour garantir la réalisation de toutes les étapes du processus et l'apport des améliorations recommandées. Nous avons toutefois noté que l'Agence a récemment mis en place un processus qui prévoit le suivi des recommandations découlant de l'évaluation de la menace et des risques posés par les nouvelles applications au bout de trois mois.

[2] Le processus de certification et d'accréditation s'intitule « processus d'évaluation de sécurité et d'autorisation » à l'ARC.

47. RECOMMANDATIONS

L'Agence du revenu du Canada devrait mettre en œuvre un processus de certification et d'accréditation assorti d'obligations en matière de reddition de comptes et de responsabilités à l'égard de la gestion clairement établies, ainsi que mettre en place des mesures de surveillance afin de garantir l'approbation en temps opportun des documents relatifs à la certification et à l'accréditation.

L'Agence devrait aussi veiller à ce que les systèmes essentiels et l'ensemble des applications connexes fassent l'objet, de façon prioritaire, d'un examen dans le cadre du processus de certification et d'accréditation, ainsi qu'à une évaluation de la menace et des risques.

Réponse de l'Agence :

L'ARC est d'accord avec ces recommandations. L'Agence a déjà mis en place un processus d'évaluation de la sécurité et continue d'y apporter des améliorations afin de suivre l'évolution des normes du Conseil du Trésor. Les processus de certification et d'accréditation actuels seront améliorés de manière à garantir que toutes les applications de l'Agence sont assujetties aux mesures d'évaluation de la sécurité suivantes :

- *En ce qui concerne les futures applications de l'organisation, le lancement d'un nouveau processus d'évaluation de la sécurité et d'autorisation conforme à la Norme du Conseil du Trésor garantira que les nouvelles applications feront l'objet d'une série complète d'activités de certification et d'accréditation. Ce processus sera mis en œuvre d'ici mars 2014.*
- *Pour ce qui est des applications existantes de l'organisation, l'ARC dresse un bilan annuel de l'état de toutes les évaluations de la sécurité réalisées depuis 2008. Un examen de toutes les applications existantes est en cours, et la priorité est accordée à l'achèvement des évaluations de la sécurité en suspens. Le calendrier pour l'achèvement des évaluations de la sécurité en suspens (pour les applications jugées hautement prioritaires) sera établi d'ici le mois de mars 2014.*
- *En ce qui a trait aux applications locales, une application Web qui répertorie les applications locales a été mise en œuvre afin de garantir que des évaluations de la sécurité adéquates sont menées et font l'objet d'un suivi conformément au processus de gouvernance amélioré décrit dans la réponse à la recommandation au paragraphe 55 ci-dessous.*

Des applications locales sont souvent mises en œuvre sans avoir été examinées et approuvées au préalable

48. Une application locale est un logiciel utilisé pour satisfaire à un besoin ou régler un problème local ou régional de nature administrative.

49. D'importantes préoccupations au sujet des contrôles actuels pour les applications locales ont été soulevées dans le cadre d'une vérification interne menée par l'ARC en 2007. À l'époque, les propriétaires des applications ne suivaient pas toujours les politiques et les procédures applicables aux applications locales. L'enregistrement des applications locales dans un répertoire ainsi que la consignation des renseignements importants à leur sujet n'avaient pas lieu en temps opportun, ce qui signifie que l'information contenue dans le répertoire n'était pas à jour. En outre, certaines applications locales avaient été mises en œuvre avant d'avoir fait l'objet de l'examen et de l'approbation obligatoires.

50. L'ARC a effectué un suivi de sa vérification de 2007 en 2010. Elle a ensuite donné aux employés des bureaux régionaux la consigne d'enregistrer toutes les applications locales dans le répertoire. Ce répertoire central devait comprendre une liste à jour des applications locales ainsi que les renseignements importants concernant leur examen, les recommandations formulées à leur égard et leur approbation par des employés de l'Agence autorisés.

51. Lors de notre vérification, nous nous attendions à constater que l'Agence avait pleinement mis en œuvre des politiques et des procédures pour gérer les applications locales, comme le préconisaient les recommandations formulées à la suite des vérifications de 2007 et de 2010. Nous avons constaté que les employés de l'Agence interviewés connaissaient et comprenaient bien les politiques relatives aux applications locales, et que des progrès avaient été réalisés depuis 2010 au chapitre de l'amélioration de la gestion des applications locales.

52. Nous avons toutefois cerné des problèmes persistants sur les plans de la gestion du répertoire et du respect des politiques et des procédures de l'Agence en ce qui a trait aux applications locales. Bien que des efforts aient été déployés récemment pour corriger la situation dans l'un des bureaux que nous avons visités, nous avons constaté que l'information enregistrée dans le répertoire n'est pas tenue à jour : le répertoire contient des coordonnées désuètes et des renseignements inexacts sur l'état, et un certain nombre d'applications locales utilisées dans les divers bureaux régionaux n'y figurent pas.

53. Nous avons aussi observé des retards importants pour ce qui est de l'examen et de l'approbation des applications locales. Nous avons examiné le dossier de onze applications locales et constaté que neuf d'entre elles utilisaient des renseignements personnels; de ce nombre, huit étaient toujours en attente d'approbation de deux à quatre ans après leur mise en œuvre et n'avaient pas subi les contrôles obligatoires de la sécurité et de la qualité.

54. En l'absence d'un examen de la sécurité et d'une approbation à l'étape de la conception d'une solution locale, la mise en œuvre d'une application pourrait compromettre involontairement la confidentialité des renseignements sur les contribuables. L'ARC a informé le Commissariat que les directions générales de l'Agence donnent maintenant la priorité à l'enregistrement et au contrôle de la sécurité des applications locales afin de réduire l'arriéré actuel.

55. RECOMMANDATIONS

L'Agence du revenu du Canada devrait :

- s'assurer que ses politiques, pratiques et procédures en matière de gestion des applications locales sont suivies et que des mesures de sécurité adéquates sont appliquées pour protéger les renseignements sur les contribuables que contiennent ces applications;
- veiller à ce que le répertoire des applications locales fasse régulièrement l'objet d'un examen pour garantir l'exhaustivité, l'exactitude et la fiabilité de l'information qu'il contient;
- assurer un suivi à chaque étape des processus d'examen et d'assurance de la qualité, et veiller à ce que toutes les applications locales soient approuvées par des employés autorisés avant d'être mises en œuvre.

Réponse de l'Agence :

L'ARC est d'accord avec ces recommandations. La réalisation d'un examen des procédures et des mesures de sécurité actuelles, assorti d'une évaluation de l'état actuel du répertoire des applications locales, devrait être achevée d'ici la fin de juillet 2013. Un plan d'action sera mis en place d'ici la fin de septembre 2013 pour combler les lacunes décelées.

Le processus de gouvernance sera amélioré; il comprendra dorénavant un processus obligatoire d'examen et d'approbation visant à confirmer que des évaluations des facteurs relatifs à la vie privée et des examens des aspects techniques de la sécurité sont réalisés avant la mise en œuvre des applications, afin d'assurer l'exhaustivité, l'exactitude et la fiabilité de l'information à leur sujet. D'ici la fin de septembre 2013, tous les propriétaires d'applications locales seront informés des améliorations apportées en ce qui a trait à la surveillance de la gestion des applications.

ACCÈS DES EMPLOYÉS AUX RENSEIGNEMENTS ET SURVEILLANCE DE L'UTILISATION QU'ILS EN FONT

56. Les organisations conçoivent et mettent en œuvre des mécanismes de contrôle de l'accès et de surveillance des employés afin de prévenir, de limiter et de détecter les cas d'accès non autorisé aux renseignements personnels de nature délicate des clients. Ces mécanismes de contrôle de l'accès interne comprennent notamment une protection par mots de passe, l'identification et l'authentification des utilisateurs, et la surveillance de l'activité des utilisateurs. Utilisées ensemble lorsqu'ils fonctionnent comme prévu, ces mesures limitent les possibilités que des employés consultent, utilisent ou communiquent de façon inappropriée des renseignements personnels.

57. Notre vérification a porté plus particulièrement sur les mécanismes de contrôle interne visant à gérer les droits d'accès des employés ainsi que sur la surveillance de l'accès électronique aux données des contribuables par les employés.

L'ARC travaille actuellement à renforcer les mécanismes de contrôle relatifs aux droits d'accès

58. Selon la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI) du Conseil du Trésor, l'attribution et la suppression dans les règles des accès électroniques sont essentielles pour garantir que les données sont consultées en fonction du besoin de connaître. Particulièrement :

    - les employés doivent faire l'objet d'une vérification de la sécurité avant d'être autorisés à consulter les données;
    - l'accès doit être restreint aux seules données dont les personnes ont besoin pour s'acquitter de leurs fonctions;
    - les droits d'accès doivent être revus régulièrement pour s'assurer qu'ils correspondent aux responsabilités et au statut de l'employé;
    - les privilèges d'accès doivent être supprimés lorsque les employés quittent l'organisation ou s'en absentent pendant une longue période de temps;
    - les privilèges d'accès doivent être modifiés lorsque les employés passent à un emploi qui ne nécessite pas le même niveau d'accès.

59. Nous nous attendions à constater que l'ARC avait mis en œuvre des processus et des procédures pour accorder, supprimer et gérer l'accès des employés aux systèmes qui traitent les données des contribuables. Nous avons examiné les processus et les procédures utilisés par l'Agence pour établir le niveau et les privilèges d'accès de chaque employé, et pour les modifier lorsque les fonctions d'un employé changent ou que ce dernier quitte l'organisation.

60. Nous avons constaté que l'Agence dispose d'une politique de contrôle de l'accès et fait appel à un système de révision des accès des employés (SRAE) pour définir et tenir à jour les privilèges d'accès des employés. Les privilèges relatifs aux TI sont conférés à chaque employé selon ses fonctions particulières, lesquelles peuvent changer selon la charge de travail et d'autres facteurs. Les gestionnaires revoient les privilèges d'accès au moins deux fois par année au moyen du SRAE et d'autres outils connexes. Ils les vérifient et les modifient aussi, au besoin, en cas de changement aux fonctions d'un employé.

61. Les entrevues que nous avons menées nous ont permis d'observer que les gestionnaires et les chefs d'équipe responsables de l'examen et de l'approbation des privilèges d'accès des employés connaissent le processus relatif au SRAE et considèrent ce dernier comme un outil efficace de gestion des accès. Des suggestions ont été faites en vue de la simplification du processus et d'une plus grande connectabilité entre le SRAE et les systèmes d'information sur les ressources humaines. Le fait d'établir des liens avec les renseignements sur les employés pourrait faciliter la vérification du statut d'emploi et la mise à jour des privilèges d'accès des employés.

62. L'Agence travaille actuellement à la mise en œuvre d'un projet multiphase et pluriannuel de gestion de l'identité et de l'accès visant l'amélioration des mécanismes de contrôle et des processus relatifs à l'attribution, à la modification et à la suppression des privilèges d'accès des employés. L'ARC s'attend à automatiser et à renforcer davantage le processus de révision des accès au cours des prochaines années.

63. RECOMMANDATION

L'Agence du revenu du Canada devrait continuer d'apporter des améliorations aux mécanismes de contrôle de son système de gestion de l'identité et de l'accès de façon à veiller à ce que l'accès des employés se limite aux renseignements nécessaires pour l'exercice de leurs fonctions, selon le principe du besoin de connaître.

Réponse de l'Agence :

L'ARC accepte la recommandation et s'appuiera sur les travaux qui ont été menés à bien à ce jour dans le cadre du projet de la gestion de l'identité et de l'accès, notamment en ce qui a trait aux ressources d'information, dont la création a été achevée en mars 2012, et au dépôt de référence en matière d'identité, qui a été mis en œuvre en mai 2013. L'ARC s'engage par ailleurs à :

- *poursuivre les travaux en cours pour l'examen des rôles et des profils utilisés par les gestionnaires pour attribuer l'accès à leurs employés, tâche qui sera menée à bien d'ici octobre 2014;*
- *mettre en œuvre un processus amélioré de vérification annuelle, tâche qui sera menée à bien d'ici décembre 2014;*
- *poursuivre la mise en œuvre des étapes résiduelles du projet et du programme de gestion de l'identité et de l'accès.*

À ce jour, l'ARC a investi quelque 10,5 M$ et prévoit effectuer d'autres investissements d'envergure afin de s'attaquer à la question dans le cadre des projets de gestion de l'identité et de l'accès ainsi que du système national de piste de vérification.

Les identifiants d'utilisateur génériques ne sont pas contrôlés de façon adéquate

64. Les mécanismes de contrôle de l'accès aux fins de l'identification et de l'authentification des utilisateurs du système sont des outils très importants parce que bien d'autres mesures de protection reposent sur eux. La norme en matière de GSTI du Conseil du Trésor oblige toutes les institutions fédérales à mettre en œuvre des mesures de protection de l'identification et de l'authentification pour tous les réseaux et tous les systèmes. Les mesures de contrôle mises en œuvre doivent correspondre au niveau de risque inhérent des réseaux ou des systèmes de l'organisation. Les institutions doivent aussi s'assurer que l'identité des employés a été confirmée avant qu'un identifiant unique d'utilisateur du système leur soit attribué.

65. Un identifiant d'utilisateur générique (identifiant générique) est un identifiant qui est utilisé par plusieurs personnes. Ces identifiants sont utilisés pour des processus de système et l'accès partagé à certaines fonctions. Le personnel des TI les utilise aussi pour la mise au point, la mise à l'essai et l'entretien des systèmes. Les identifiants génériques permettent à plus d'un employé des TI de vérifier la fonctionnalité d'un système sans qu'il soit nécessaire de modifier ou d'élargir l'accès conféré à leur identifiant personnel.

66. L'utilisation d'identifiants génériques entraîne toutefois des risques en matière de reddition de comptes et de protection de la vie privée. Quand les institutions ont recours à des identifiants génériques, il leur est difficile de vérifier qui a consulté tel ou tel système. Lorsqu'un identifiant générique a été utilisé pour entrer dans un système, on ne peut retracer immédiatement l'employé en cause. Ces identifiants sont souvent utilisés dans des environnements d'essai non opérationnels[3], mais il est quand même possible que des données de nature délicate sur les contribuables s'y trouvent.

67. Nous nous attendions à constater que l'ARC avait mis en œuvre des mécanismes de contrôle pour gérer et limiter l'utilisation des identifiants génériques par les employés. Selon la norme relative à l'identification des utilisateurs de l'Agence, les identifiants doivent correspondre à une seule personne. L'ARC a élaboré une norme relative à l'administration des comptes génériques et des procédures connexes pour gérer les exceptions lorsque les besoins opérationnels exigent l'utilisation d'identifiants génériques.

68. Nous nous sommes penchés sur l'utilisation qui est faite des identifiants génériques au sein de l'Agence et nous avons constaté que ceux-ci font l'objet d'un contrôle limité. Nous avons aussi constaté que l'Agence possède plus de 10 000 identifiants génériques, mais ses registres n'indiquent pas toujours clairement si ces identifiants sont utilisés, par qui et à quelles fins.

69. Selon la politique de l'ARC, les identifiants génériques doivent être autorisés par la direction et approuvés par la Direction de la technologie de l'information avant leur utilisation. Nous avons cependant constaté qu'ils ne font pas l'objet d'un suivi central et qu'un bon nombre d'identifiants génériques plus anciens n'ont pas été approuvés. L'ARC a confirmé que les rapports produits au sujet des identifiants génériques ne sont pas examinés pour gérer l'utilisation de ces derniers.

70. RECOMMANDATIONS

L'Agence du revenu du Canada devrait examiner les identifiants génériques existants afin de déterminer s'ils sont nécessaires, si leur utilisation a été autorisée et s'ils font l'objet d'un contrôle. Elle devrait par ailleurs supprimer tous les identifiants qui ne sont pas utilisés.

L'Agence du revenu du Canada devrait aussi veiller à ce que tous les identifiants génériques soient assujettis aux processus établis d'examen et d'approbation.

Réponse de l'Agence :

L'ARC accepte les recommandations et :

- *renforcera le processus en vigueur en mettant en œuvre des mécanismes de contrôle améliorés qui permettront de réduire considérablement le nombre de comptes génériques créés. Cette tâche sera menée à bien d'ici décembre 2013.*
- *tirera parti du dépôt de référence en matière d'identité mis en œuvre en mai 2013 pour réaliser un examen complet de tous les comptes génériques existants. Elle prendra ensuite les mesures qui s'imposent, dont la suppression des comptes qui ne sont plus utilisés, et attribuera la responsabilité de chaque compte à des employés précis. Cette tâche sera menée à bien d'ici mars 2014.*
- *améliorera les mesures de sensibilisation à la sécurité et de reddition de comptes en ce qui a trait aux comptes génériques. Cette tâche sera menée à bien d'ici décembre 2014.*

[3] Le personnel des TI a recours à des environnements d'essai non opérationnels pour mettre au point et mettre à l'essai des systèmes avant qu'ils ne soient utilisés pour traiter des déclarations de revenus dans le cadre des activités courantes de l'Agence.

Des lacunes existent en ce qui a trait à la surveillance de l'accès aux renseignements des contribuables par les employés

71. Pour établir les responsabilités de chacun, surveiller le respect des politiques en matière de sécurité et faire enquête en cas d'infraction, il faut être en mesure de déterminer les interventions effectuées dans les systèmes de TI, le moment où elles ont eu lieu ainsi que la ou les personnes en cause. Pour ce faire, les institutions utilisent des logiciels qui créent une piste de vérification, soit un journal ou un registre des interventions effectuées par un employé dans un système.

72. Nous nous attendions à constater que l'ARC avait mis en place des politiques et des procédures en ce qui a trait à la journalisation des pistes de vérification et à l'examen des registres ainsi créés. Tous les systèmes qui permettent aux employés d'accéder à des renseignements concernant des contribuables devraient être munis de processus de journalisation des pistes de vérification. Les journaux de vérification devraient également faire l'objet d'une surveillance continue et des avis devraient être communiqués en temps opportun lorsqu'on soupçonne qu'un employé accède à des renseignements de façon inappropriée. Nous avons examiné les procédures de l'ARC pour ce qui est de la surveillance de l'accès par les employés et nous avons évalué la mise en œuvre des processus de surveillance.

73. L'Agence a établi la Politique pour la journalisation et la surveillance de l'accès aux renseignements des contribuables. Selon la politique de l'ARC sur la journalisation des pistes de vérification, l'accès de tous les employés à ses systèmes doit être consigné — sous réserve d'exceptions limitées. L'ARC a installé des outils qui lui permettent de suivre et de surveiller l'accès aux données des contribuables par les employés sur la majorité de ses systèmes.

74. Le système national de piste de vérification de l'ARC comporte deux volets :

- Le système de piste de vérification en ligne est l'outil principal de surveillance de l'Agence et permet aux gestionnaires investis de pouvoirs délégués d'effectuer des vérifications aléatoires de l'accès aux renseignements des contribuables par les employés au cours d'une période d'un à sept jours. Tout résultat indiquant un accès potentiellement inapproprié est signalé à la Division des affaires internes et sécurité (DAIS) pour la conduite d'une enquête.
- Le système de piste de vérification consigne les données sur l'historique d'accès. Les gestionnaires peuvent demander que soit produit un rapport de piste de vérification à la suite du dépôt d'une plainte par un contribuable, à l'appui d'une enquête relative à des allégations ou à des soupçons d'accès non autorisé, ou en réponse à une demande au titre de l'accès à l'information ou de la protection de la vie privée. L'accès aux données du SPV est contrôlé par la DAIS.

75. En 2010, l'ARC a mené des vérifications visant à établir si les pistes de vérification produites par le système étaient enregistrées, gérées et surveillées conformément à sa politique en la matière. Ces vérifications internes ont révélé que la politique de journalisation de l'ARC ne renfermait pas suffisamment de directives à l'intention des gestionnaires quant à l'utilisation des pistes de vérification pour surveiller l'accès des employés, et ont permis de cerner l'existence d'une lacune dans les mécanismes de contrôle du système qui permettent de donner suite aux résultats obtenus lors des examens des pistes de vérification, de les surveiller ou d'en faire rapport, et ce, peut importe où l'on se trouve à l'ARC.

76. Selon la politique sur la journalisation des pistes de vérification, les gestionnaires et les chefs d'équipe doivent procéder régulièrement à l'examen, à l'aide du système de piste de vérification en ligne, de l'accès de tous les employés qui relèvent d'eux. Ces examens ont pour but de repérer les cas d'accès inhabituels ou inappropriés par des employés et, le cas échéant, de fournir des éléments d'information en vue d'une enquête.

77. Nous avons constaté l'existence d'un manque d'uniformité dans la façon dont les gestionnaires, aux bureaux que nous avons visités, effectuaient leurs examens des pistes de vérification en ligne. Parmi les personnes interviewées, peu avaient reçu une formation en bonne et due forme sur la conduite des examens. Un bon nombre trouvaient la procédure complexe, longue et essentiellement inefficace. Même si le processus d'examen des pistes de vérification en ligne pourrait dissuader les employés de consulter de manière inappropriée les renseignements de contribuables, pour les gestionnaires interviewés, il représentait rarement le principal moyen de détecter les accès non autorisés.

78. Nous avons aussi constaté que l'efficacité des mécanismes de contrôle de l'Agence pour détecter et prévenir l'accès non autorisé aux renseignements des contribuables et l'utilisation de ceux-ci à des fins inappropriées est limitée par l'absence d'un outil automatisé permettant de relever et de signaler les accès suspects aux systèmes.

79. Même si la politique mise en place par l'Agence prévoit que toutes les consultations de renseignements de contribuables doivent être consignées, nous avons constaté que certaines des applications de l'ARC ne produisent pas de piste de vérification.

80. L'Agence nous a fait part de ses plans pour accroître l'efficacité de son système de surveillance des pistes de vérification en ligne et pour signaler plus rapidement les accès inhabituels ou à haut risque à ses gestionnaires dans ses nouveaux rapports de journal de vérification. L'ARC est également en train d'évaluer des options pour le renforcement du système de piste de vérification au moyen d'une surveillance continue et proactive des interventions des employés.

81. RECOMMANDATION

L'Agence du revenu du Canada devrait continuer de renforcer ses systèmes et ses processus de journalisation des pistes de vérification, et y incorporer des outils d'évaluation du risque pour signaler toute intervention suspecte de la part d'un employé.

Réponse de l'Agence :

L'ARC accepte la recommandation et continuera de renforcer son système et ses processus de journalisation des pistes de vérification en :

- *terminant la mise en œuvre du nouvel outil d'analyse des registres des pistes de vérification afin d'aider les gestionnaires à passer en revue les accès des employés aux systèmes, tâche qui sera menée à bien d'ici décembre 2013;*
- *poursuivant les travaux en cours en vue de l'amélioration des outils technologiques et des processus opérationnels connexes permettant d'analyser de manière proactive les interventions des utilisateurs, de permettre un dépistage précoce des problèmes et de détecter certains types de comportements.*

Comme il est mentionné dans la réponse de l'ARC à la recommandation figurant au paragraphe 63 (plus haut), à ce jour, l'ARC a investi quelque 10,5 M$ et prévoit faire d'autres investissements d'envergure afin de s'attaquer à la question dans le cadre des projets de la gestion de l'identité et de l'accès et de la modernisation du système national de piste de vérification.

L'accès aux renseignements des contribuables par les concepteurs des TI ne fait pas l'objet d'une surveillance adéquate

82. Les renseignements des contribuables sont copiés dans des environnements d'essai non opérationnels (voir note 3 au bas de la page 19) dans le cadre de la mise au point, de la mise à l'essai et de l'entretien des systèmes de TI de l'Agence. Par exemple, l'ARC télécharge un sous-ensemble de données de contribuables chaque année. Cette démarche permet au personnel des TI de mettre au point et de mettre à l'essai les modifications aux systèmes requises en prévision du prochain cycle fiscal, sans perturber les opérations fiscales courantes de l'ARC.

83. Certains membres de l'équipe de conception des TI jouissent d'un accès en mode lecture seulement aux renseignements des contribuables dans des environnements opérationnels. Ce type d'accès est approuvé afin de permettre aux concepteurs de régler des problèmes concernant des dossiers d'impôt précis. Nous nous attendions à constater que les politiques et les procédures générales de l'ARC régissant l'accès aux renseignements des contribuables s'appliquaient également aux concepteurs de TI.

84. L'accès par les concepteurs aux systèmes et aux données dans les environnements d'essai et opérationnels est contrôlé au moyen de profils qui sont attribués en fonction des exigences de chaque poste et du principe du besoin de connaître. Les droits d'accès sont examinés deux fois l'an pour ces utilisateurs au moyen du SRAE.

85. Les pistes de vérification dans les environnements d'essai enregistrent l'accès par les employés des TI aux renseignements des contribuables. Cependant, elles ne sont conservées que pendant cinq jours, ce qui limite la capacité de l'Agence d'assurer le suivi à cet égard. De plus, les pistes de vérification produites dans les environnements d'essai ne sont pas incorporées au système national de piste de vérification de l'Agence.

86. Des membres spécialement désignés des équipes de conception sont aussi autorisés à transférer les renseignements des contribuables d'un environnement opérationnel à un environnement d'essai. L'information enregistrée par le système permet de savoir quel employé a procédé au téléchargement, mais rien n'indique quels comptes de contribuables ont été téléchargés.

87. RECOMMANDATIONS

L'Agence du revenu du Canada devrait s'assurer que des mesures adéquates sont mises en œuvre pour atténuer les risques liés à l'accès, par les concepteurs, aux renseignements des contribuables dans des environnements d'essai.

L'Agence du revenu du Canada devrait également contrôler, suivre et surveiller rigoureusement les transferts de renseignements de contribuables d'environnements opérationnels à des environnements d'essai.

Réponse de l'Agence :

L'ARC accepte les recommandations. L'ARC augmentera les contrôles liés à l'utilisation des renseignements de contribuables dans les environnements d'essai en :

- *modernisant et en diffusant ses politiques concernant les transferts et l'accès aux renseignements des contribuables dans les environnements d'essai, tâche qui sera menée à bien d'ici mars 2014;*
- *procédant à l'analyse des options disponibles afin de faire ressortir la méthode la plus efficace pour contrôler, suivre et surveiller les transferts de renseignements de contribuables d'un environnement opérationnel à un environnement d'essai. L'analyse sera menée à bien d'ici mars 2014, et l'option approuvée sera mise en œuvre immédiatement après.*

ATTEINTES À LA VIE PRIVÉE

88. Selon les Lignes directrices sur les atteintes à la vie privée du Conseil du Trésor :

> « Une atteinte à la vie privée suppose la collecte, l'usage, la communication, la conservation ou le retrait inappropriés ou non autorisés de renseignements personnels. […] Une atteinte à la vie privée peut être le résultat d'erreurs de bonne foi ou d'actes malveillants commis par des employés, des tiers, des partenaires d'ententes de partage d'information ou des intrus ».

89. Les Lignes directrices encouragent les institutions fédérales à dresser un plan pour contrer les atteintes à la vie privée qui comporte les éléments suivants : prévention des risques, limitation et atténuation des répercussions des atteintes, réalisation d'une analyse des causes de l'incident, et mise en œuvre de mesures correctives pour éviter des problèmes semblables à l'avenir.

Pièce 3 : Mesures à prendre en cas d'atteinte à la vie privée

Bureaux de première responsabilité

1. Prendre des mesures immédiates pour réprimer l'atteinte et protéger les dossiers, systèmes ou sites Web touchés.
2. Consigner l'atteinte.
3. Aviser le coordonnateur de l'accès à l'information et de la protection des renseignements personnels (AIPRP) et l'agent de sécurité du Ministère puisque la plupart des atteintes à la vie privée supposent une infraction à la sécurité.

Agents de sécurité et coordonnateurs de l'AIPRP du Ministère

4. Selon le processus établi à l'institution, le coordonnateur de l'AIPRP ou le fonctionnaire responsable de la sécurité doit aviser l'administrateur général et la Direction des communications.

suite…

5. Mener une enquête interne et formuler des recommandations afin d'éviter une répétition de l'incident.

Coordonnateurs de l'AIPRP

6. Aviser le Commissariat à la protection de la vie privée […]. L'institution doit aviser le CPVP de l'atteinte le plus tôt possible après en avoir pris connaissance (en dedans de quelques jours).
7. Aviser les personnes dont les renseignements personnels ont été communiqués à tort, volés ou perdus […]. L'institution doit aviser les personnes touchées de l'atteinte dans les meilleurs délais pour leur permettre de prendre des mesures de protection ou d'atténuer les préjudices causés par le vol d'identité ou les autres torts possibles.
8. Suivi.

Source : Lignes directrices du Conseil du Trésor sur les atteintes à la vie privée, 8 août 2012.

90. Nous nous attendions à constater que l'ARC avait mis en œuvre un processus lui permettant de satisfaire aux attentes du Conseil du Trésor. Conformément à la recommandation que nous avons formulée dans notre vérification de 2009 des cadres de gestion de la protection de la vie privée, nous nous attendions aussi à ce qu'une entente d'échange des renseignements concernant le signalement des atteintes à la vie privée ait été conclue entre la Direction des affaires internes et de la prévention de la fraude (AIPF) et la Direction de l'accès à l'information et de la protection des renseignements personnels.

Des mécanismes pour la réalisation d'enquêtes sur les atteintes à la vie privée ont été mis en place

91. Notre examen des dossiers nous a permis de constater que la Direction des affaires internes et de la securité (DAIS) réalise des enquêtes approfondies sur les atteintes à la vie privée. Les entrevues que nous avons menées avec des gestionnaires et des chefs d'équipe ont confirmé que ceux-ci savent en quoi consiste une atteinte à la vie privée, savent comment et à qui la signaler, et connaissent le rôle qu'ils doivent jouer dans les processus de signalement et d'enquête.

92. En réponse à la recommandation que nous avons formulée lors de notre vérification de 2009, l'ARC a mis en place un protocole d'entente sur l'échange de renseignements concernant les atteintes à la vie privée (le Protocole) en avril 2010. Le Protocole décrit les fonctions dont doivent s'acquitter les responsables de la sécurité et du bureau de l'AIPRP en cas d'atteinte.

Le bureau de l'AIPRP n'est pas régulièrement informé des atteintes

93. Les Lignes directrices sur les atteintes à la vie privée du Conseil du Trésor (Lignes directrices du CT) renferment des conseils à l'intention des ministères et des organismes sur le signalement des atteintes à la vie privée et le suivi à effectuer :

> « Il importe de mettre le coordonnateur de l'AIPRP et l'agent de sécurité du ministère (ASM) à contribution, pour que la protection de la vie privée et la sécurité des biens soient prises en compte dans le processus de résolution. [...] Le bureau de l'AIPRP du ministère doit également procéder à une évaluation afin de mettre au jour les faiblesses en gestion des renseignements personnels. L'évaluation et les recommandations connexes devraient porter sur les problèmes qui ne sont pas strictement liés à des problèmes de sécurité ».

94. Le protocole sur les atteintes de l'ARC prévoit que, lorsque des atteintes internes visent des renseignements personnels et risquent de causer des préjudices à une personne, la Direction des affaires internes et de la securité (DAIS) doit en informer le directeur de l'AIPRP conformément aux résultats d'une évaluation du risque. Le protocole n'oblige toutefois pas la Direction à signaler toutes les atteintes à la vie privée au bureau de l'AIPRP.

95. Notre examen des dossiers sur les atteintes et des listes d'enquêtes menées sur des atteintes fournis par l'Agence nous a permis de constater que la Direction des affaires internes et de la securité (DAIS) n'informe pas régulièrement le bureau de l'AIPRP des atteintes à la vie privée. Or, si le bureau de l'AIPRP n'est pas informé des atteintes, il ne peut pas jouer son rôle en ce qui a trait au signalement et à l'analyse des atteintes ainsi qu'à la réalisation d'un suivi à leur sujet.

96. D'après nos propres dossiers, le Commissariat est aussi rarement informé par l'Agence des atteintes causées par l'accès non autorisé d'employés à des renseignements de contribuables et par la communication non autorisée de ces derniers. De plus, les dossiers de l'ARC sur les atteintes n'indiquent pas les raisons pour lesquelles l'Agence a décidé de ne pas informer les contribuables concernés et le Commissariat des atteintes à la vie privée. Cela dit, l'ARC a récemment instauré un processus d'évaluation du risque qui comprend la consignation des raisons pour lesquelles les contribuables concernés et le Commissariat devraient ou ne devraient pas être informés.

De graves atteintes concernant la communication de renseignements de contribuables ont eu lieu à l'Agence

97. La consultation d'une liste d'enquêtes internes menées par l'ARC en 2011 et 2012 a révélé l'existence de plus de 50 enquêtes concernant un accès non autorisé aux renseignements de contribuables. Notre examen d'un échantillon de ces enquêtes nous a permis de constater qu'un bon nombre concernaient aussi la communication non autorisée de renseignements de contribuables. Certaines enquêtes portaient sur l'accès par des employés à des milliers de dossiers de contribuables pendant une période prolongée sans que personne ne remarque quoi que ce soit.

98. Les dossiers de l'Agence concernant les atteintes découlant d'accès et de communications non autorisés indiquent que les employés fautifs étaient motivés par la curiosité, l'intérêt personnel, le désir d'accorder un traitement préférentiel et des visées frauduleuses. Dans les cas où il a été établi qu'il s'agissait d'actes malveillants de la part d'employés, des sanctions disciplinaires ont été imposées, allant de l'avertissement au congédiement.

99. RECOMMANDATION

Conformément aux Lignes directrices sur les atteintes à la vie privée du Conseil du Trésor, l'Agence du revenu du Canada devrait s'assurer que la Direction de l'accès à l'information et de la protection des renseignements personnels est informée de toutes les atteintes dès leur détection.

Réponse de l'Agence :

L'ARC accepte la recommandation et continue d'améliorer son protocole d'échange de renseignements en :

- *élargissant immédiatement la portée du Protocole pour inclure le signalement de toutes les atteintes conformément aux Lignes directrices sur les atteintes à la vie privée du Conseil du Trésor;*
- *Veillant au signalement plus rapide des atteintes à la Direction de l'accès à l'information et de la protection des renseignements personnels.*

Conclusion

100. La *Loi sur la protection des renseignements personnels* impose des obligations aux institutions fédérales en ce qui a trait au respect du droit à la vie privée des Canadiennes et des Canadiens.

101. Il règne, à l'ARC, une culture de sécurité et de confidentialité qui est attribuable à la présence d'un cadre d'intégrité, de politiques, d'activités de formation et de sensibilisation, ainsi que d'autres initiatives. On décèle toutefois des lacunes prononcées sur le plan de la mise en œuvre et de la surveillance de certaines de ses principales politiques et pratiques en matière de sécurité et de protection de la vie privée. Ces lacunes nuisent à la capacité de l'ARC de protéger pleinement les renseignements sur les contribuables contre toute consultation, utilisation ou communication inappropriée. Plus particulièrement, on constate :

- qu'afin de respecter une recommandation formulée lors de la vérification de 2009, un chef de la protection des renseignements personnels (CPRP) a été nommé le 3 avril 2013. Le rôle du CPRP n'a cependant pas encore été défini avec précision aux fins de la coordination des obligations relatives à la reddition de comptes, aux responsabilités et aux activités liées à la protection de la vie privée à l'échelle de l'Agence;
- que des évaluations des facteurs relatifs à la vie privée ne sont pas toujours réalisées afin d'évaluer les risques associés à des changements relatifs aux programmes qui auront des répercussions sur les renseignements personnels des contribuables;
- que de nombreux systèmes informatiques qui traitent des renseignements sur les contribuables ne font pas l'objet d'une évaluation de la menace et des risques, ce qui pourrait faire en sorte que des lacunes ne soient pas décelées;
- que l'efficacité des contrôles mis en œuvre par l'Agence afin de repérer et de prévenir toute consultation ou utilisation inappropriée de renseignements sur les contribuables par des employés est limitée par l'absence d'un outil automatisé permettant de repérer et de signaler les potentiels cas d'accès inapproprié ainsi que par certaines lacunes au chapitre de la collecte de données permettant d'établir une piste de vérification dans les systèmes informatiques de l'ARC;
- que des cas d'accès inapproprié aux dossiers de milliers de contribuables sont passés inaperçus pendant une longue période;
- que la Direction de l'accès à l'information et de la protection des renseignements personnels n'est pas régulièrement informée des atteintes à la vie privée résultant de la consultation et de la communication inappropriée de renseignements sur les contribuables.

102. Depuis la parution du rapport portant sur la dernière vérification effectuée par le Commissariat, en 2009, l'ARC a effectué des progrès en ce qui a trait au renforcement de ses politiques et de ses procédures en matière de sécurité et de protection de la vie privée, ainsi qu'en ce qui concerne la communication de ses attentes à l'égard de la protection des renseignements personnels à ses employés. L'Agence déploie également des efforts en vue d'améliorer la gestion des droits d'accès et de surveiller plus étroitement l'accès des employés aux renseignements sur les contribuables.

103. Les observations et les recommandations formulées dans le présent rapport ont pour but d'améliorer les pratiques de traitement des renseignements personnels de l'Agence et, ainsi, d'atténuer les risques de consultation, d'utilisation ou de communication non autorisée des renseignements personnels des contribuables.

À propos de la vérification

AUTORISATION LÉGISLATIVE

L'article 37 de la *Loi sur la protection des renseignements personnels* confère à la commissaire à la protection de la vie privée l'autorisation d'examiner les pratiques de traitement des renseignements personnels des institutions fédérales.

OBJECTIF

La vérification visait à déterminer si l'Agence du revenu du Canada a mis en place des contrôles suffisants pour protéger les renseignements personnels des contribuables, et si ses politiques, ses procédures et ses processus de gestion des renseignements personnels des contribuables sont conformes aux principes relatifs à l'équité dans le traitement de l'information établis aux articles 4 à 8 de la *Loi sur la protection des renseignements personnels*.

CRITÈRES

Les critères de vérification ont été établis en se fondant sur la *Loi sur la protection des renseignements personnels* ainsi que sur les politiques, les directives et les normes du Secrétariat du Conseil du Trésor qui portent sur la gestion des renseignements personnels.

Nous nous attendions à constater que l'Agence :

- avait mis en place des mesures de protection appropriées pour protéger les renseignements personnels qui lui avaient été confiés;
- avait établi des responsabilités claires pour la protection des renseignements personnels au sein de son organisation;
- avait établi un mécanisme de conformité pour assurer le respect de ses obligations en vertu de la *Loi sur la protection des renseignements personnels*;
- avait mis en place un cadre assurant le recensement et l'atténuation des risques liés à la protection de la vie privée associés aux systèmes, aux programmes et aux activités;
- avait élaboré et mis en œuvre un mécanisme de signalement des atteintes à la vie privée et d'intervention à cet égard;
- avait fait en sorte que ses employés soient conscients de leurs responsabilités et de leurs obligations en ce qui a trait au respect du droit à la vie privée des contribuables;
- avait mis en œuvre les recommandations formulées dans le rapport de 2009 de la commissaire à la protection de la vie privée sur les cadres de gestion de la protection de la vie privée dans certaines institutions fédérales.

PORTÉE ET DÉMARCHE

La vérification comprenait un examen des cadres, des politiques, des procédures, des processus, des systèmes, des contrôles administratifs et des mesures de protection techniques en matière de responsabilisation et de gestion du risque régissant l'accès des employés aux renseignements personnels des contribuables canadiens ainsi que leur utilisation.

La vérification ne comprenait pas un examen des pratiques de gestion des renseignements personnels liés à l'imposition des clients commerciaux, à la taxe sur les produits et services, à la taxe de vente harmonisée ou aux opérations liées à la taxe d'accise. Elle ne portait pas non plus sur des aspects comme l'accès de tiers aux renseignements concernant des contribuables donnés, l'accès des contribuables aux services de l'Agence par Internet et le récent transfert de certains services de TI à Services partagés Canada.

La vérification portait sur les pratiques et les procédures mises en place par l'ARC pour la gestion et la protection des renseignements personnels des contribuables. Pendant la vérification, des éléments de preuve ont été obtenus à partir de l'examen de dossiers, d'entrevues avec 101 gestionnaires, de démonstrations de systèmes et d'autres tests de vérification. Les activités de vérification ont été menées à l'administration centrale de l'Agence à Ottawa ainsi que dans les centres fiscaux régionaux de Shawinigan (Québec), de Sudbury (Ontario), de Surrey (région du Pacifique) et de Winnipeg (région des Prairies).

La vérification a débuté le 13 juillet 2012 et a été en grande partie achevée le 31 mars 2013.

NORMES

La vérification a été effectuée conformément au mandat législatif, aux pratiques et aux politiques du Commissariat à la protection de la vie privée du Canada, et respectait l'esprit des normes de vérification recommandées par l'Institut Canadien des Comptables Agréés.

ÉQUIPE DE VÉRIFICATION

Supervision :
Commissaire adjointe, Chantal Bernier

Vérificateurs :
Tom Fitzpatrick
Gaétan Létourneau
Anne Overton
Rick Smith
Bryony Townsend
Matt Williams

Annexe A – Liste des recommandations

Gestion de la protection de la vie privée et responsabilité à cet égard	
RECOMMANDATION	**RÉPONSE DE L'AGENCE**
L'Agence du revenu du Canada devrait définir avec précision le rôle du chef de la protection des renseignements personnels et surveiller la mise en œuvre de son mandat en ce qui a trait à la sensibilisation des employés à la protection des renseignements personnels, à la réduction du risque d'atteinte à la vie privée et au respect global de la ***Loi sur la protection des renseignements personnels*** par l'Agence.	Comme le souligne le rapport, la ***Loi sur la protection des renseignements personnels*** n'oblige pas les institutions fédérales à nommer un chef de la protection des renseignements personnels, et les politiques du Conseil du Trésor ne définissent pas le rôle de ce dernier. Néanmoins, l'Agence du revenu du Canada (ARC) est d'accord avec la recommandation et a nommé un chef de la protection des renseignements personnels qui est chargé de la surveillance de la gestion de la protection de la vie privée à l'Agence en avril 2013. Le chef de la protection des renseignements personnels fait partie du Comité de direction de l'Agence et s'est vu confier le vaste mandat d'assurer la protection de la vie privée à l'Agence, notamment : • en exerçant un droit de regard sur les décisions relatives à la protection des renseignements personnels, y compris les évaluations des facteurs relatifs à la vie privée; • en défendant le droit à la vie privée des particuliers conformément aux lois et aux politiques en vigueur, ce qui comprend la gestion des cas d'atteinte à la vie privée au sein de l'Agence — une responsabilité qu'il partage avec l'équipe de la Sécurité; • en supervisant la sensibilisation au respect de la vie privée à l'Agence au moyen de la mise sur pied de diverses activités de communication et de formation. Le chef de la protection des renseignements personnels, qui assure la liaison avec le Commissariat à la protection de la vie privée, surveillera le respect global de la ***Loi sur la protection des renseignements personnels*** par l'Agence et fera rapport à la haute direction de la situation au chapitre de la gestion de la protection de la vie privée au sein de l'organisation au moins deux fois par année financière.
Conformément à la Directive du Conseil du Trésor sur les évaluations des facteurs relatifs à la vie privée, l'Agence du revenu du Canada devrait réaliser, examiner et approuver une évaluation des facteurs relatifs à la vie privée avant la mise en œuvre de tout nouveau programme ou initiative susceptible de mettre en péril la confidentialité des renseignements sur les contribuables.	L'ARC est d'accord avec la recommandation et veillera à ce qu'une évaluation des facteurs relatifs à la vie privée soit réalisée, examinée et approuvée avant la mise en œuvre de tout nouveau programme ou initiative susceptible de mettre en péril la confidentialité des renseignements sur les contribuables. Pour s'acquitter de cette obligation, le chef de la protection des renseignements personnels s'est vu confier la responsabilité globale de surveiller l'état d'avancement des EFVP, conformément à son mandat. Il vérifiera aussi régulièrement que les cadres supérieurs de l'organisation s'acquittent de leur responsabilité à l'égard de la réalisation d'EFVP et en fera rapport au commissaire et à la haute direction.

Sécurité des technologies de l'information	
RECOMMANDATION	**RÉPONSE DE L'AGENCE**
L'Agence du revenu du Canada devrait mettre en œuvre un processus de certification et d'accréditation assorti d'obligations en matière de reddition de comptes et de responsabilités à l'égard de la gestion clairement établies, ainsi que mettre en place des mesures de surveillance afin de garantir l'approbation en temps opportun des documents relatifs à la certification et à l'accréditation. L'Agence devrait aussi veiller à ce que les systèmes essentiels et l'ensemble des applications connexes fassent l'objet, de façon prioritaire, d'un examen dans le cadre du processus de certification et d'accréditation, ainsi qu'à une évaluation de la menace et des risques.	L'ARC est d'accord avec ces recommandations. L'Agence a déjà mis en place un processus d'évaluation de la sécurité et continue d'y apporter des améliorations afin de suivre l'évolution des normes du Conseil du Trésor. Les processus de certification et d'accréditation actuels seront améliorés de manière à garantir que toutes les applications de l'Agence sont assujetties aux mesures d'évaluation de la sécurité suivantes : • En ce qui concerne les futures applications de l'organisation, le lancement d'un nouveau processus d'évaluation de la sécurité et d'autorisation conforme à la Norme du Conseil du Trésor garantira que les nouvelles applications feront l'objet d'une série complète d'activités de certification et d'accréditation. Ce processus sera mis en œuvre d'ici mars 2014. • Pour ce qui est des applications existantes de l'organisation, l'ARC dresse un bilan annuel de l'état de toutes les évaluations de la sécurité réalisées depuis 2008. Un examen de toutes les applications existantes est en cours, et la priorité est accordée à l'achèvement des évaluations de la sécurité en suspens. Le calendrier pour l'achèvement des évaluations de la sécurité en suspens (pour les applications jugées hautement prioritaires) sera établi d'ici le mois de mars 2014. • En ce qui a trait aux applications locales, une application Web qui répertorie les applications locales a été mise en œuvre afin de garantir que des évaluations de la sécurité adéquates sont menées et font l'objet d'un suivi conformément au processus de gouvernance amélioré décrit dans la réponse à la recommandation au paragraphe 55 ci-dessous.
L'Agence du revenu du Canada devrait : • s'assurer que ses politiques, pratiques et procédures en matière de gestion des applications locales sont suivies et que des mesures de sécurité adéquates sont appliquées pour protéger les renseignements sur les contribuables que contiennent ces applications; • veiller à ce que le répertoire des applications locales fasse régulièrement l'objet d'un examen pour garantir l'exhaustivité, l'exactitude et la fiabilité de l'information qu'il contient; • assurer un suivi à chaque étape des processus d'examen et d'assurance de la qualité, et veiller à ce que toutes les applications locales soient approuvées par des employés autorisés avant d'être mises en œuvre.	L'ARC est d'accord avec ces recommandations. La réalisation d'un examen des procédures et des mesures de sécurité actuelles, assorti d'une évaluation de l'état actuel du répertoire des applications locales, devrait être achevée d'ici la fin de juillet 2013. Un plan d'action sera mis en place d'ici la fin de septembre 2013 pour combler les lacunes décelées. Le processus de gouvernance sera amélioré; il comprendra dorénavant un processus obligatoire d'examen et d'approbation visant à confirmer que des évaluations des facteurs relatifs à la vie privée et des examens des aspects techniques de la sécurité sont réalisés avant la mise en œuvre des applications, afin d'assurer l'exhaustivité, l'exactitude et la fiabilité de l'information à leur sujet. D'ici la fin de septembre 2013, tous les propriétaires d'applications locales seront informés des améliorations apportées en ce qui a trait à la surveillance de la gestion des applications.

Accès des employés aux renseignements et surveillance de l'utilisation qu'ils en font	
RECOMMANDATION	**RÉPONSE DE L'AGENCE**
L'Agence du revenu du Canada devrait continuer d'apporter des améliorations aux mécanismes de contrôle de son système de gestion de l'identité et de l'accès de façon à veiller à ce que l'accès des employés se limite aux renseignements nécessaires pour l'exercice de leurs fonctions, selon le principe du besoin de connaître.	L'ARC accepte la recommandation et s'appuiera sur les travaux qui ont été menés à bien à ce jour dans le cadre du projet de la gestion de l'identité et de l'accès, notamment en ce qui a trait aux ressources d'information, dont la création a été achevée en mars 2012, et au dépôt de référence en matière d'identité, qui a été mis en œuvre en mai 2013. L'ARC s'engage par ailleurs à : • poursuivre les travaux en cours pour l'examen des rôles et des profils utilisés par les gestionnaires pour attribuer l'accès à leurs employés, tâche qui sera menée à bien d'ici octobre 2014; • mettre en œuvre un processus amélioré de vérification annuelle, tâche qui sera menée à bien d'ici décembre 2014; • poursuivre la mise en œuvre des étapes résiduelles du projet et du programme de gestion de l'identité et de l'accès. À ce jour, l'ARC a investi quelque 10,5 M$ et prévoit effectuer d'autres investissements d'envergure afin de s'attaquer à la question dans le cadre des projets de gestion de l'identité et de l'accès ainsi que du système national de piste de vérification.
L'Agence du revenu du Canada devrait examiner les identifiants génériques existants afin de déterminer s'ils sont nécessaires, si leur utilisation a été autorisée et s'ils font l'objet d'un contrôle. Elle devrait par ailleurs supprimer tous les identifiants qui ne sont pas utilisés. L'Agence du revenu du Canada devrait aussi veiller à ce que tous les identifiants génériques soient assujettis aux processus établis d'examen et d'approbation.	L'ARC accepte les recommandations et : • renforcera le processus en vigueur en mettant en œuvre des mécanismes de contrôle améliorés qui permettront de réduire considérablement le nombre de comptes génériques créés. Cette tâche sera menée à bien d'ici décembre 2013. • tirera parti du dépôt de référence en matière d'identité mis en œuvre en mai 2013 pour réaliser un examen complet de tous les comptes génériques existants. Elle prendra ensuite les mesures qui s'imposent, dont la suppression des comptes qui ne sont plus utilisés, et attribuera la responsabilité de chaque compte à des employés précis. Cette tâche sera menée à bien d'ici mars 2014. • améliorera les mesures de sensibilisation à la sécurité et de reddition de comptes en ce qui a trait aux comptes génériques. Cette tâche sera menée à bien d'ici décembre 2014.

RECOMMANDATION	RÉPONSE DE L'AGENCE
L'Agence du revenu du Canada devrait continuer de renforcer ses systèmes et ses processus de journalisation des pistes de vérification, et y incorporer des outils d'évaluation du risque pour signaler toute intervention suspecte de la part d'un employé.	L'ARC accepte la recommandation et continuera de renforcer son système et ses processus de journalisation des pistes de vérification en : • terminant la mise en œuvre du nouvel outil d'analyse des registres des pistes de vérification afin d'aider les gestionnaires à passer en revue les accès des employés aux systèmes, tâche qui sera menée à bien d'ici décembre 2013; • poursuivant les travaux en cours en vue de l'amélioration des outils technologiques et des processus opérationnels connexes permettant d'analyser de manière proactive les interventions des utilisateurs, de permettre un dépistage précoce des problèmes et de détecter certains types de comportements. Comme il est mentionné dans la réponse de l'ARC à la recommandation figurant au paragraphe 63 (plus haut), à ce jour, l'ARC a investi quelque 10,5 M$ et prévoit faire d'autres investissements d'envergure afin de s'attaquer à la question dans le cadre des projets de la gestion de l'identité et de l'accès et de la modernisation du système national de piste de vérification.
L'Agence du revenu du Canada devrait s'assurer que des mesures adéquates sont mises en œuvre pour atténuer les risques liés à l'accès, par les concepteurs, aux renseignements des contribuables dans des environnements d'essai. L'Agence du revenu du Canada devrait également contrôler, suivre et surveiller rigoureusement les transferts de renseignements de contribuables d'environnements opérationnels à des environnements d'essai.	L'ARC accepte les recommandations. L'ARC augmentera les contrôles liés à l'utilisation des renseignements de contribuables dans les environnements d'essai en : • modernisant et en diffusant ses politiques concernant les transferts et l'accès aux renseignements des contribuables dans les environnements d'essai, tâche qui sera menée à bien d'ici mars 2014; • procédant à l'analyse des options disponibles afin de faire ressortir la méthode la plus efficace pour contrôler, suivre et surveiller les transferts de renseignements de contribuables d'un environnement opérationnel à un environnement d'essai. L'analyse sera menée à bien d'ici mars 2014, et l'option approuvée sera mise en œuvre immédiatement après.

Atteintes à la vie privée	
RECOMMANDATION	**RÉPONSE DE L'AGENCE**
Conformément aux Lignes directrices sur les atteintes à la vie privée du Conseil du Trésor, l'Agence du revenu du Canada devrait s'assurer que la Direction de l'accès à l'information et de la protection des renseignements personnels est informée de toutes les atteintes dès leur détection.	L'ARC accepte la recommandation et continue d'améliorer son protocole d'échange de renseignements en : • élargissant immédiatement la portée du Protocole pour inclure le signalement de toutes les atteintes conformément aux Lignes directrices sur les atteintes à la vie privée du Conseil du Trésor; • veillant au signalement plus rapide des atteintes à la Direction de l'accès à l'information et de la protection des renseignements personnels.