Health Canada and the Public Health Agency of Canada
Santé Canada et l'Agence de la santé publique du Canada
Canada

Audit de la gestion des pratiques de protection des renseignements personnels à Santé Canada et à l'Agence de la santé publique du Canada

Rapport définitif

novembre 2019

Table des matières

LISTE DES ACRONYMES II
RÉSUMÉ ..... **ERROR! BOOKMARK NOT DEFINED.**
A. INTRODUCTION 1
1. Contexte 1
B. CONSTATATIONS, RECOMMANDATIONS ET RÉPONSES DE LA DIRECTION 2
1. Cadre de gestion 2
2. Évaluations des facteurs relatifs à la vie privée et protocoles de protection des renseignements personnels 3
3. Atteintes à la vie privée 5
4. Mesures de contrôle 5
5. Analyse comparative fondée sur le sexe et le genre plus 7
C. CONCLUSION 8
ANNEXE A – SECTEURS D'INTÉRÊT ET CRITÈRES 9
ANNEXE B – À PROPOS DE L'AUDIT 10
1. Objectif de l'audit 10
2. Portée de l'audit 10
3. Stratégie d'audit 10
4. Déclaration de conformité 11

LISTE DES ACRONYMES

ACSG+	Analyse comparative fondée sur le sexe et le genre plus
CT	Conseil du Trésor
AIPRP	Accès à l'information et protection des renseignements personnels
ASPC	Agence de la santé publique du Canada
CGPRP	Cadre de gestion de la protection des renseignements personnels
DGPRP	Division de la gestion de la protection des renseignements personnels
DPISG	Direction de la planification, de l'intégration et des services de gestion
EFVP	Évaluation des facteurs relatifs à la vie privée
PPRP	Protocole de protection des renseignements personnels
SC	Santé Canada

Résumé

Qu'avons-nous examiné?

Nous avons examiné les pratiques en matière de gestion de la protection des renseignements personnels à Santé Canada (SC) et à l'Agence de la santé publique du Canada (ASPC). Tous les employés sont responsables de la protection des renseignements personnels, mais la Division de la gestion de la protection des renseignements personnels (DGPRP), qui fait partie de la Direction générale des services de gestion (DGSG) de SC, dirige la coordination globale des mesures de protection des renseignements personnels pour SC et l'ASPC. Les responsabilités de la DGPRP comprennent l'élaboration de politiques, de procédures et de pratiques en matière de protection des renseignements personnels; la prestation de programmes de formation et de sensibilisation à la protection des renseignements personnels auprès du personnel; l'évaluation des atteintes à la vie privée et la production de rapports à ce sujet; la coordination de l'information fournie par SC et l'ASPC pour Info Source; et la présentation d'analyses et de conseils sur la protection des renseignements personnels à l'aide d'un certain nombre d'outils, y compris les évaluations des facteurs relatifs à la vie privée (EFVP) et les protocoles de protection des renseignements personnels.

Cet audit n'a pas visé la façon dont les directions générales s'acquittent de leurs responsabilités d'évaluer et de gérer leurs propres risques liés à la protection des renseignements personnels dans la prestation de leurs programmes ou services. Nous avons également exclu la gestion des demandes d'accès à l'information et de protection des renseignements personnels (AIPRP).

Pourquoi les pratiques de protection des renseignements personnels sont-elles importantes?

SC et l'ASPC comptent sur les renseignements personnels qu'ils détiennent au sujet des Canadiens, et la protection de ces renseignements est vitale. Les atteintes à la vie privée pourraient nuire aux Canadiens et à la réputation organisationnelle de SC et de l'ASPC. Cet audit a porté sur l'efficacité de la protection des renseignements personnels et fournit à la haute direction du Ministère et de l'Agence des recommandations sur la façon de mieux protéger les renseignements personnels à SC et à l'ASPC.

Qu'avons-nous constaté?

Nous avons constaté que des mesures de contrôle clés étaient généralement en place et fonctionnaient comme prévu pour protéger efficacement les renseignements personnels.

Nous avons constaté que les mesures de contrôle étaient adéquates dans les secteurs suivants :

- SC et l'ASPC disposent d'un cadre de gestion de la protection des renseignements personnels (CGPRP) pour décrire leurs rôles et responsabilités et orienter leurs travaux;
- Un processus approprié est en place pour la gestion des atteintes à la vie privée;
- Les évaluations des facteurs relatifs à la vie privée (EFVP) et les protocoles de protection des renseignements personnels (PPRP) sont préparés et approuvés par les programmes et sont examinés par la DGPRP.

Nous avons constaté des faiblesses dans les mesures de contrôle dans les secteurs suivants :

- En l'absence d'une gestion des risques appropriée, la DGPRP fonctionnait avec peu de renseignements organisationnels et, par conséquent, ses efforts de sensibilisation étaient principalement axés sur les secteurs les plus à risque au sein de sa propre direction générale, plutôt que sur les risques à l'échelle de SC et de l'ASPC;
- Bien que les EFVP et les PPRP aient été préparés et approuvés pour atténuer les risques d'atteinte à la vie privée, les recommandations formulées par la DGPRP dans les évaluations ne faisaient pas l'objet d'une surveillance par la DGPRP;
- Bien que certains membres du personnel de la DGPRP aient reçu une formation sur l'analyse comparative fondée sur le sexe et le genre plus (ACSG+), la DGPRP n'avait pas documenté une analyse de la prise en compte de l'ACSG+ dans ses processus.

L'audit contient quatre recommandations qui aideront à renforcer collectivement les pratiques de gestion de la protection des renseignements personnels à SC et à l'ASPC.

A. Introduction

1. Contexte

1. La *Loi sur la protection des renseignements personnels* régit les pratiques des institutions fédérales concernant le traitement des renseignements personnels. La *Loi*, qui est entrée en vigueur le 1er juillet 1983, limite la collecte, l'utilisation, le partage et la divulgation des renseignements personnels des personnes. Au sens de la *Loi*, les renseignements personnels sont des renseignements, quels que soient leur forme et leur support, qui concernent une personne et qui peuvent être utilisés seuls ou en combinaison avec d'autres renseignements afin d'identifier une personne.
2. Le Commissariat à la protection de la vie privée du Canada surveille le respect de la *Loi sur la protection des renseignements personnels* et aide les institutions fédérales à améliorer leurs pratiques de traitement de renseignements personnels. La Division de la gestion de la protection des renseignements personnels (DGPRP) et la Division de l'accès à l'information et de la protection des renseignements personnels (AIPRP) gèrent les exigences de la *Loi sur la protection des renseignements personnels* pour Santé Canada (SC) et l'Agence de la santé publique du Canada (ASPC). Ces services partagés relèvent de la Direction de la planification, de l'intégration et des services de gestion (DPISG) de la Direction générale des services de gestion de SC.
3. SC et l'ASPC gèrent une grande quantité de renseignements personnels sur la santé des Canadiens. Bien que la DGPRP et la Division de l'AIPRP soient principalement responsables de l'administration de la *Loi sur la protection des renseignements personnels*, la protection des renseignements personnels est en fin de compte une responsabilité partagée entre tous les employés de SC et de l'ASPC.

B. Constatations, recommandations et réponses de la direction

1. Cadre de gestion

4. Nous nous attendions à ce que SC et l'ASPC aient mis en place une approche de gestion des risques pour la protection des renseignements personnels, notamment un mécanisme qui permettrait la détermination et la présentation directe de commentaires par les directions générales quant à leurs risques liés à la protection des renseignements personnels. Il serait ainsi possible de définir un univers de risques liés à la protection des renseignements personnels qui aiderait la Division de la gestion de la protection des renseignements personnels (DGPRP) à cibler les activités de sensibilisation dans les deux organisations.

5. La DGPRP a mis à jour le Cadre de gestion de la protection des renseignements personnels (CGPRP) de SC et de l'ASPC en 2019 dans le contexte de ses efforts de renouvellement. Le CGPRP a défini les rôles et les responsabilités liés à la protection des renseignements personnels pour les principaux intervenants dans l'ensemble des organisations et a présenté cinq piliers clés pour une gestion efficace de la protection des renseignements personnels. La gestion efficace des risques a été identifiée comme l'un des cinq piliers clés du CGPRP. Toutefois, ce pilier n'a pas été plus développé pour établir comment la DGPRP assurerait une gestion efficace des risques, ni comment la DGPRP établirait son univers de risques liés à la protection des renseignements personnels pour favoriser une gestion ministérielle efficace de ces risques.

6. Nous avons constaté que la DGPRP avait élaboré des lignes directrices et des outils[1] pour fournir des conseils et aider les directions générales à déterminer les risques liés à la protection des renseignements personnels pour des programmes ou des initiatives en particulier et à en faire rapport à la DGPRP. La DGPRP a également formulé des recommandations sur la façon d'atténuer ces risques particuliers. L'examen de ces évaluations distinctes de la protection des renseignements personnels par la DGPRP lui a donné l'occasion d'acquérir des connaissances sur les divers risques liés à la protection des renseignements personnels dans l'ensemble des organisations. Nous avons également constaté que la DGPRP avait eu de nombreuses conversations ponctuelles sur les risques liés à la protection des renseignements personnels avec les divers programmes qui communiquaient avec elle pour obtenir des conseils. Cela a permis à la DGPRP d'obtenir une foule de renseignements sur les risques liés à la protection des renseignements personnels. Toutefois, il n'y a pas eu de collecte ni de priorisation de ces évaluations et conversations dans un univers de risques liés à la protection des renseignements personnels.

7. Dans l'ensemble, SC et l'ASPC avaient un CGPRP indiquant la nécessité d'une gestion efficace des risques. Toutefois, ils n'avaient pas d'approche ministérielle de gestion des risques pour évaluer et gérer les risques liés à la protection des renseignements personnels au niveau du ministère et de la direction générale. Bien qu'aucune évaluation n'ait été effectuée au niveau de la direction générale, la DGPRP a dirigé des activités axées sur les risques qui sont mentionnées dans son plan provisoire de mobilisation stratégique. SC et l'ASPC profiteraient de l'établissement d'un univers plus stratégique de risques liés à la protection des renseignements personnels afin de mieux éclairer les

[1] Par exemple : Trousse d'évaluation des facteurs relatifs à la vie privée, Guide sur la protection des renseignements personnels, Rapport sur les incidents relatifs à la protection des renseignements personnels, CGPRP et Guide sur la protection des renseignements personnels lors de la passation de marchés.

activités de la DGPRP, y compris les interventions ciblées et les campagnes de formation et de sensibilisation.

Recommandation 1

La sous-ministre adjointe, Direction générale des services de gestion, devrait renforcer les pratiques de gestion des risques de la direction générale en effectuant une évaluation des risques de l'Agence et du Ministère avec la rétroaction de toutes les directions générales.

Réponse de la direction

La direction accepte la recommandation.

La direction continuera de s'appuyer sur les discussions ciblées qui ont lieu actuellement, ainsi que sur les rapports sur les risques liés à la protection des renseignements personnels qui sont produits par l'entremise des tableaux de bord trimestriels aux comités exécutifs de SC et de l'ASPC.

Les mesures prévues tiennent compte du fait que les cadres supérieurs et les hauts fonctionnaires des programmes qui traitent les renseignements personnels sont responsables de leur traitement conforme[1].

1. Directive sur les pratiques relatives à la protection de la vie privée. Articles 6.2 et 6.3

2. Évaluations des facteurs relatifs à la vie privée et protocoles de protection des renseignements personnels

8. Les évaluations des facteurs relatifs à la vie privée (EFVP) servent à déterminer les risques potentiels liés à la protection des renseignements personnels associés aux programmes ou services nouveaux ou considérablement modifiés qui recueillent des renseignements personnels à des fins administratives (c.-à-d., lorsqu'une décision est prise au sujet d'une personne). Elles recommandent également un plan pour éliminer ou atténuer ces risques à un niveau acceptable. Les protocoles de protection des renseignements personnels (PPRP) sont établis pour les programmes ou les initiatives qui ont des répercussions sur la protection des renseignements personnels pour la collecte non administrative de renseignements personnels (c.-à-d., les renseignements personnels recueillis à des fins de recherche, d'audit ou d'évaluation, à des fins statistiques ou dans le cadre de la prestation du programme).
9. Nous nous attendions à ce que des processus existent et soient utilisés efficacement pour la préparation des EFVP et des PPRP. Nous nous attendions également à ce que les EFVP et les PPRP soient approuvés et conformes à la *Directive sur l'évaluation des facteurs relatifs à la vie privée*.
10. Nous avons constaté que les EFVP et les PPRP avaient été préparés et approuvés pour atténuer les risques liés à la protection des renseignements personnels. Des processus appropriés étaient en place pour la réalisation des EFVP et des PPRP, et étaient conformes aux politiques et aux lignes directrices pertinentes.

11. Étant donné que les EFVP et les PPRP sont lancés au niveau du programme, il est possible qu'il y ait des lacunes lorsque les programmes ne sont pas au courant de leurs responsabilités ou des mesures qu'ils doivent prendre. La DGPRP a pris l'initiative d'aider à déterminer les répercussions sur la protection des renseignements personnels pour les programmes ou les initiatives qui n'étaient peut-être pas au courant de leurs responsabilités. Cela s'est fait principalement en examinant les mémoires au Cabinet (MC) et les présentations au Conseil du Trésor pour les deux organisations, ainsi qu'en participant aux processus de planification des investissements de SC.
12. Nous nous attendions également à ce que SC et l'ASPC surveillent la mise en œuvre des recommandations formulées par la DGPRP et des stratégies d'atténuation des risques liés à la protection des renseignements personnels élaborées par le programme dans les EFVP et les PPRP.
13. Nous avons constaté qu'il n'y avait pas de processus de suivi des EFVP et des PPRP au niveau des directions générales. Nous n'avons trouvé aucune preuve que la DGPRP ou une tierce partie a surveillé la mise en œuvre des stratégies d'atténuation des risques décrites dans les EFVP et les PPRP dans toutes les directions générales.
14. Dans l'ensemble, les EFVP et les PPRP ont été préparés et approuvés pour atténuer les risques et se conformer aux politiques du CT. Toutefois, aucun processus n'était en place pour surveiller la mise en œuvre des activités d'atténuation des risques dans toutes les directions générales.

Recommandation 2

La sous-ministre adjointe, Direction générale des services de gestion, devrait surveiller et suivre les recommandations de la Division de la gestion de la protection des renseignements personnels concernant les évaluations des facteurs relatifs à la vie privée et les protocoles de protection des renseignements personnels.

Réponse de la direction

La direction accepte la recommandation.

Les mesures prévues tiennent compte du fait que les cadres supérieurs et les hauts fonctionnaires des programmes qui traitent les renseignements personnels sont responsables de leur traitement conforme[2].

2. Directive sur les pratiques relatives à la protection de la vie privée. Articles 6.2 et 6.3

3. Atteintes à la vie privée

15. Une atteinte à la vie privée suppose la collecte, l'usage, la divulgation, la conservation ou l'élimination inappropriée de renseignements personnels. Une atteinte à la vie privée peut se produire au sein d'une organisation ou hors site et peut être le résultat d'erreurs de bonne foi ou d'actes malveillants commis par des employés, des tierces partis, des partenaires d'ententes de partage d'information ou des intrus. Le Secrétariat du Conseil du Trésor (SCT) fournit aux ministères des Lignes directrices sur les atteintes à la vie privée ainsi qu'une Trousse d'outils pour la gestion des atteintes à la vie privée. Les processus ministériels relatifs aux atteintes à la vie privée doivent respecter la *Politique sur la protection de la vie privée* et la *Directive sur les pratiques relatives à la protection de la vie privée* du CT.

16. Nous nous attendions à trouver des politiques ou des lignes directrices ministérielles qui décrivent les modalités de détermination, de signalement, d'enquête et de correction pour les atteintes possibles à la vie privée, et à ce que ces politiques soient conformes aux directives pertinentes du CT. Nous nous attendions également à ce que des processus soient en place pour assurer le suivi des rapports d'atteinte à la vie privée et des plans d'atténuation, ainsi que pour surveiller les tendances en matière d'atteinte à la vie privée.

17. Nous avons constaté que la DGPRP avait créé et distribué des lignes directrices ministérielles, des procédures opérationnelles normalisées et des listes de vérification pour aider les programmes, ainsi que pour guider ses propres opérations internes sur la façon de traiter les atteintes à la vie privée. L'examen des documents nous a permis de constater que ces ressources correspondaient aux exigences du CT.

18. Nous nous attendions à ce que les rapports complets sur les atteintes à la vie privée soient conformes aux politiques du CT et du Ministère, et nous avons constaté que c'était le cas.

19. Dans l'ensemble, les procédures de détermination, de déclaration, d'enquête et de correction des atteintes possibles à la vie privée étaient bien établies.

4. Mesures de contrôle

20. Bien que la DGPRP soit le centre d'expertise pour les conseils aux programmes et pour aider les directions générales à se conformer à la *Loi sur la protection des renseignements personnels*, la protection des renseignements personnels est en fin de compte la responsabilité des programmes, ainsi que de tous les employés de SC et de l'ASPC. Par conséquent, la sensibilisation des employés est une mesure de contrôle clé pour la protection des renseignements personnels.

21. Nous nous attendions à ce que SC et l'ASPC aient une stratégie de sensibilisation à la protection des renseignements personnels visant à faire de la protection des renseignements personnels une partie intégrante de la culture de travail et des valeurs fondamentales qui guident tous les employés et gestionnaires de SC et de l'ASPC. Nous nous attendions également à ce que SC et l'ASPC aient élaboré des documents de formation pertinents sur la protection des renseignements personnels à la disposition de tous les employés et gestionnaires, et à ce qu'il existe des campagnes de formation et de sensibilisation pour aider les employés à demeurer au courant de leurs rôles et responsabilités en vertu de la *Loi sur la protection des renseignements personnels*.

22. Nous avons constaté que les efforts de sensibilisation des dernières années avaient donné lieu à une mobilisation limitée et rarement à des résultats concrets. Les efforts des dernières années ont été décrits comme étant insuffisamment adaptés et orientés pour prioriser et répondre aux besoins particuliers des secteurs présentant des risques élevés pour la protection des renseignements personnels. Nous avons constaté que la DGPRP avait récemment mis à l'essai ses nouveaux outils et ses nouvelles directives de formation et de sensibilisation. Toutefois, ces activités étaient principalement axées sur les secteurs présentant le risque le plus élevé au sein de sa propre direction générale, plutôt que sur les risques à l'échelle de SC et de l'ASPC.

23. Nous avons constaté que la DGPRP participait à des activités de promotion, comme des communications par des bulletins de nouvelles et un kiosque pendant la Semaine nationale de la fonction publique. Cependant, aucun des cours de formation sur la protection des renseignements personnels de la DGPRP n'était obligatoire à l'échelle de l'organisation. La protection des renseignements personnels faisait autrefois partie de la formation initiale des nouveaux employés, mais elle a été retirée de la formation obligatoire au moment de l'intégration.

24. La DGPRP a mené des activités de formation sur la protection des renseignements personnels au Laboratoire national de microbiologie et, à la suite d'une sensibilisation accrue, le nombre de questions sur la protection des renseignements personnels adressées à la DGPRP a augmenté. Cela souligne l'importance d'une formation continue de sensibilisation.

25. Nous avons constaté que la DGPRP élaborait un plan de mobilisation stratégique qui vise à utiliser une approche fondée sur le risque pour les communications internes, dans le but d'améliorer la sensibilisation à la protection des renseignements personnels et les pratiques de SC et de l'ASPC qui sont perçues comme étant les plus à risque.

26. Dans l'ensemble, nous avons trouvé des lacunes dans les efforts de sensibilisation. La DGPRP s'ait servi d'une ébauche de plan de mobilisation et ses efforts ont principalement été axés sur les secteurs les plus à risque au sein de sa propre direction générale. SC et l'ASPC gagneraient à accroître leurs efforts de sensibilisation en fonction des risques dans les deux organisations.

Recommandation 3

La sous-ministre adjointe, Direction générale des services de gestion, devrait finaliser et mettre en œuvre le plan de mobilisation stratégique de la Division de la gestion de la protection des renseignements personnels, afin de mettre en œuvre intégralement sa stratégie de formation et de sensibilisation dans l'ensemble des deux organisations de façon stratégique et fondée sur les risques.

Réponse de la direction

La direction accepte la recommandation.

Le plan de mobilisation stratégique est utilisé depuis décembre 2018 pour déterminer les secteurs présentant le risque le plus élevé. Il a par la suite permis à la DGPRP de prioriser son travail de mobilisation au niveau du Ministère et de l'Agence.

Les directions générales de SC et de l'Agence gèrent divers types et quantités de renseignements personnels en fonction de leur mandat; par conséquent, les mesures décrites seront priorisées en tenant compte des évaluations des risques propres aux directions générales.

5. Analyse comparative fondée sur le sexe et le genre plus

27. Nous nous attendions à ce que le personnel de la DGPRP ait suivi la formation sur l'analyse comparative fondée sur le sexe et le genre plus (ACSG+) et que l'ACSG+ ait été intégrée aux processus opérationnels de la DGPRP, le cas échéant[2].

28. Nous avons constaté que trois membres du personnel de la DGPRP sur dix-huit avaient suivi la formation sur l'ACSG+. L'une de ces trois personnes possède une connaissance approfondie de l'ACSG+. Nous avons constaté que la DGPRP avait effectué une analyse de la façon dont l'ACSG+ pourrait être intégrée aux processus opérationnels de la DGPRP.

29. En conclusion, bien que certains membres du personnel de la DGPRP aient reçu une formation sur l'ACSG+, la DGPRP n'avait pas documenté une analyse de la prise en compte de l'ACSG+ dans ses processus.

Recommandation 4

La sous-ministre adjointe, Direction générale des services de gestion, devrait veiller à ce que tout le personnel de la Division de la gestion de la protection des renseignements personnels ait suivi la formation de base sur l'analyse comparative fondée sur le sexe et le genre plus et évaluer si l'ACSG+ peut être pertinente pour ses pratiques et outils opérationnels.

Réponse de la direction

La direction accepte la recommandation.

[2] Nous n'avons pas tenu compte de l'ACSG+ à l'extérieur de la DGPRP et de la façon dont les considérations liées à l'ACSG+ sont prises en compte dans le traitement des renseignements personnels par les programmes. Toutefois, cette considération fait partie du rendement des audits du BAE lors de l'audit d'un programme particulier.

C. Conclusion

30. L'objectif de cet audit était de déterminer si les renseignements personnels sont protégés efficacement à SC et à l'ASPC.

31. Nous avons constaté que des mesures de contrôle clés étaient généralement en place et fonctionnaient comme prévu pour protéger efficacement les renseignements personnels.

32. Nous avons constaté que les mesures de contrôle étaient adéquates dans les secteurs suivants :

- SC et l'ASPC disposent d'un cadre de gestion de la protection des renseignements personnels (CGPRP) pour décrire leurs rôles et responsabilités et orienter leurs travaux;
- Un processus approprié est en place pour la gestion des atteintes à la vie privée;
- Les évaluations des facteurs relatifs à la vie privée (EFVP) et les protocoles de protection des renseignements personnels (PPRP) sont préparés et approuvés par les programmes et sont examinés par la DGPRP, conformément à la *Politique sur la protection de la vie privée* du Conseil du Trésor (CT).

33. Nous avons constaté des faiblesses dans les mesures de contrôle dans les secteurs suivants :

- SC et l'ASPC n'ont pas de cadre documenté de gestion des risques pour la protection des renseignements personnels dans leurs organisations. En l'absence d'une gestion des risques appropriée, la DGPRP fonctionnait avec peu de renseignements organisationnels et, par conséquent, ses efforts de sensibilisation étaient principalement axés sur sa propre direction générale, plutôt que sur les risques;

- Bien que les EFVP et les PPRP aient été préparés et approuvés pour atténuer les risques d'atteinte à la vie privée, les recommandations formulées par la DGPRP dans les évaluations ne faisaient pas l'objet d'une surveillance systématique;

- Bien que certains membres du personnel de la DGPRP aient reçu une formation sur l'ACSG+, la DGPRP n'avait pas documenté une analyse de la prise en compte de l'ACSG+ dans ses processus.

34. L'audit contient quatre recommandations qui aideront à renforcer collectivement les pratiques de gestion de la protection des renseignements personnels à SC et à l'ASPC.

Annexe A – Secteurs d'intérêt et critères

Audit des pratiques en matière de gestion de la protection des renseignements personnels à SC et à l'ASPC
Critères d'audit
1. SC et l'ASPC ont un cadre de gestion des risques pour évaluer et gérer les risques liés à la protection des renseignements personnels au niveau ministériel.
2. Des évaluations des facteurs relatifs à la vie privée (EFVP) et des protocoles de protection des renseignements personnels sont préparés, approuvés et surveillés afin d'atténuer les risques.
3. Les procédures permettant de repérer et de signaler les possibles atteintes à la vie privée, de faire enquête sur celles-ci et d'y remédier sont établies et fonctionnent comme prévu.
4. Des mesures de contrôle existent pour la protection des renseignements personnels.
5. Les considérations liées à l'ACSG+ sont prises en compte dans le traitement des renseignements personnels.

Annexe B – À propos de l'audit

1. Objectif de l'audit

L'objectif de l'audit est de déterminer si les renseignements personnels sont protégés efficacement à SC et à l'ASPC.

2. Portée de l'audit

La portée du présent audit incluait les principaux processus, pratiques et structures ministériels qui concernent la gestion des pratiques de protection des renseignements personnels à SC et à l'ASPC.

L'audit excluait la gestion des demandes d'AIPRP. Il excluait aussi la sécurité physique et la protection concrète des renseignements personnels (chiffrement des données et classeurs verrouillés), ainsi que le cycle de vie de la gestion de l'information (GI), puisqu'ils ont été évalués au cours d'audits récents de la sécurité physique et de la gestion de l'information.

3. Stratégie d'audit

L'audit a été effectué conformément à la *Politique sur l'audit interne* du gouvernement du Canada, par l'examen et la collecte de données suffisantes et pertinentes pour fournir une assurance raisonnable à l'appui de sa conclusion.

L'audit a permis d'examiner la conception et l'application des pratiques de gestion de la protection des renseignements personnels à SC et à l'ASPC, par rapport aux exigences de la *Loi sur la protection des renseignements personnels* ainsi que des politiques et directives connexes.

La stratégie d'audit comprenait notamment les éléments suivants :

- Examen des documents, des politiques, des normes, des lignes directrices et des cadres pertinents;
- Observations et entrevues avec les responsables clé des programmes de la DPISG et des directions générales ayant des responsabilités liées au traitement des renseignements personnels;
- Mise à l'épreuve des pratiques de gestion de la protection des renseignements personnels (mise à l'épreuve détaillée des mesures de contrôle se rapportant aux pratiques de gestion de la protection des renseignements personnels) à partir des EFVP échantillonnées, des banques de renseignements personnels, des protocoles de protection des renseignements personnels, des ententes sur l'échange de renseignements et des contrats;
- Analyse des résultats des entrevues, des demandes de renseignements, des examens des documents et des essais détaillés.

4. Déclaration de conformité

Le présent audit a été réalisé en conformité avec les *Normes internationales pour la pratique professionnelle l'audit interne* et il est validé par les résultats du Programme d'assurance et d'amélioration de la qualité du Bureau de l'audit et de l'évaluation.