Emploi et Développement social Canada | Employment and Social Development Canada

Maintenant et demain, l'excellence dans tout ce que nous entreprenons

Non-classifié

Direction générale des services de vérification interne

Audit du cadre de contrôle du Ministère pour la gestion des renseignements personnels (protection des renseignements personnels)

Août 2015

SP-1107-01-16F

Canada

Vous pouvez télécharger cette publication en ligne à : publicentre.edsc.gc.ca

Ce document est offert sur demande en médias substituts (gros caractères, braille, audio sur cassette, audio sur DC, fichiers de texte sur disquette, fichiers de texte sur DC ou DAISY) en composant le 1 800 O-Canada (1-800-622-6232). Les personnes qui utilisent un téléscripteur (ATS) doivent composer le 1-800-926-9105.

© Sa Majesté la Reine du Chef du Canada, 2016

Pour obtenir de plus amples renseignements sur les droits de reproduction : droitdauteur.copyright@HRSDC-RHDCC.gc.ca

PDF
Nº de cat. : Em20-36/2016F-PDF
ISBN : 978-0-660-04159-9

EDSC
Nº de cat. : SP-1107-01-16F

Table des matières

Sommaire exécutif 1
1.0 Renseignements généraux 4
1.1 Contexte 4
1.2 Objectif de l'audit 4
1.3 Portée 4
1.4 Méthodologie 5
2.0 Constatations de l'audit 5
2.1 Gouvernance et responsabilisation 6
2.2 Gouvernance des renseignements personnels 7
2.3 Culture, formation et sensibilisation 10
2.4 Gestion des risques 11
2.5 Assurance de la conformité 12
3.0 Conclusion 13
4.0 Énoncé d'assurance 13
Annexe A : Évaluation des critères d'audit 14
Annexe B : Glossaire 16

Sommaire exécutif

Dans le cadre des programmes d'Emploi et Développement social Canada (EDSC), il est nécessaire de recueillir, d'utiliser et de divulguer des renseignements personnels détaillés, et parfois de nature délicate. En raison de l'ampleur du mandat d'EDSC, le Ministère détient le plus grande nombre de renseignements personnels du gouvernement fédéral. Bien que la protection des renseignements personnels des Canadiens constitue une priorité ministérielle, le Ministère a été exposé en 2012 à la perte d'un disque dur externe et à une clé USB[1] contenant des renseignements personnels.

Suite à cette atteinte à la vie privée, le Commissariat à la protection de la vie privée (CPVP) a tenu une enquête et formulé des recommandations qui ont été appliquées par EDSC. Le Ministère avait déjà enclenché un processus de révision du Cadre de gestion de la protection des renseignements personnels (CGPRP), notamment par l'entremise d'une initiative pluriannuelle de renouvellement en matière de protection des renseignements personnels. Le Plan d'action pour le renouvellement de la protection des renseignements personnels incluait l'élaboration d'une nouvelle version de la Politique ministérielle sur la gestion des renseignements personnels (PMGRP), qui a été mise en œuvre le 1er avril 2014. La PMGRP et ses directives énoncent l'application de la *Loi sur la protection des renseigmenents personnels,* L.R.C (1985), ch. P-21, du Règlement sur la protection des renseignements personnels, de la *Loi sur le ministère de l'Emploi et du Développement social (MEDS)* 'Code de protection des renseignements personnels'[2], des politiques et des directives du Conseil du Trésor en matière de protection des renseignements personnels et du Code de conduite d'EDSC, de manière à favoriser un régime de politiques robuste pour la protection et l'utilisation judicieuse des renseignements personnels.

Le profil de risque du ministère (PRM) 2014-2015 d'EDSC indique que la protection et la sécurité des renseignements personnels constituent l'un des cinq principaux risques pour le Ministère. Parmi les principaux facteurs de risque, il y a le volume élevé de renseignements personnels et de nature délicate[3], le grand nombre d'ententes sur l'échange de renseignements (EER), ainsi que les méthodes et les pratiques actuelles de gestion de l'information (GI) et de protection des renseignements personnels.

Objectif de l'audit

L'objectif du présent audit visait à évaluer la pertinence et l'efficacité du CGPRP d'EDSC pour la protection des renseignements personnels des Canadiens.

Sommaire des constatations principales

- EDSC dispose d'une structure de gouvernance bien définie et fonctionnelle en appui au cadre ministériel de protection des renseignements personnels, ainsi qu'à la gestion et à la protection des renseignements personnels. Cette structure de gouvernance comprend des responsabilités bien définies et un comité consacré à la gouvernance de la gestion de la protection des renseignements personnels. Le Comité de la protection des renseignements personnels et la sécurité de l'information (CPRPSI), qui est le principal organisme de gouvernance en la matière, est perçu par les gestionnaires interviewés comme étant plutôt

---

1 USB est un sigle qui signifie Universal Serial Bus (bus série universel), un port qui peut être utilisé pour brancher du matériel à un ordinateur.

2 La Partie IV de la législation habilitante, aussi connue sous le nom de Code de protection des renseignements personnels du Ministère, applique au Ministère des règles plus sévères en matière de transmission de renseignements que la *Loi sur la protection des renseignements personnels*, L.R.C. (1985), ch. P-21 sur laquelle il a préséance.

3 Les renseignements de nature délicate sont des renseignements qui nécessitent une protection supérieure et un devoir de diligence plus rigoureux.

axé sur les transactions. Il s'agit là d'une occasion pour le CPRPSI d'agir de manière horizontale à l'égard des enjeux et des risques en matière de protection et de sécurité des renseignements personnels.

- La gestion des EER demeure un risque puisque les ententes qui renferment des dispositions sur la transmission de renseignements n'ont pas toutes été définies, évaluées et gérées.
- Les processus de gestion du risque pour les évaluations des facteurs relatifs à la vie privée (EFVP) pourraient être renforcés en vue de fournir un portrait complet des risques en matière de technologie de l'information (TI) établis dans les EER et ce, en temps opportun.
- La documentation pertinente de l'ensemble de politiques sur la protection des renseignements personnels est difficile à localiser dans les dépôts de documents sur iService[4] et dans l'intranet.
- Bien que l'agent de sécurité du Ministère (ASM) et le chef de la protection des renseignements personnels (CPRP) fassent appel à une gestion transactionnelle des incidents en matière de protection des renseignements personnels, des rapports ne sont pas produits de façon systématique en appui à une analyse efficace des tendances à l'échelle du Ministère. La production de rapports d'incidents en matière de protection des renseignements personnels et d'analyses des tendances permettrait à l'ASM, au CPRP, à la haute direction et au CPRPSI de prendre des décisions informées, stratégiques et horizontales sur les orientations du programme de protection des renseignements personnels et de valider les réussites ou les lacunes des initiatives mises en œuvre.
- La formation obligatoire en matière de protection des renseignements personnels et les efforts de communication sur la gestion de ces renseignements à l'intention des employés du Ministère se sont avérés satisfaisants. La formation sur la gestion de l'information et comportements en milieu de travail (GICMT) est considérée comme une pratique exemplaire du Ministère en ce qui concerne l'intégration des principes relatifs à la protection renseignements personnels aux principes qui touchent la TI et la GI.
- EDSC surveille le cadre de gestion des renseignements personnels, notamment en ayant en place un organisme de gouvernance spécialement affecté à cette fin et un régime d'audit interne. De la surveillance est également effectuée au moyen d'exercices tels que les plans d'action en matière de protection des renseignements personnels dirigés par les programmes (PAPRPDP).
- La surveillance des contrôles d'accès continue d'être un défi et le demeurera tant que les mesures visant à gérer les lacunes cernés dans les audits précédents ne seront pas entièrement mises en œuvre.

Conclusion de l'audit

L'audit a permis de constater que le CGPRP d'EDSC permettait de répondre adéquatement à la plupart des questions touchant la protection des renseignements personnels. Des processus et des contrôles durables sont en place, notamment un organisme de gouvernance spécial et un ensemble de politiques en matière de gestion des renseignements personnels. Cependant, certains domaines du CGPRP peuvent encore être améliorés. Des opportunités existent afin de mieux intégrer les processus de l'EFVP, de l'évaluation de la sécurité et de l'autorisation (ESA) et de l'évaluation des menaces et des risques (EMR) pour la production de rapports consolidés sur les tendances en matière d'incidents liés aux renseignements personnels et pour améliorer la gestion des EER.

Recommandations

1. Le Ministère devrait s'assurer que l'inventaire des EER soit terminé en temps opportun et que toutes les ententes renfermant des dispositions relatives à la transmission de renseignements soient définies, évaluées et gérées de manière continue.

[4] iService fait partie de l'intranet d'ESDC et comprend des renseignements à jour à l'intention des employés sur les services de première ligne.

2. En partenariat avec le secrétaire ministériel dans ses fonctions de CPRP, l'ASM devrait veiller à la mise en place d'un mécanisme visant à regrouper les rapports sur les incidents liés à la protection des renseignements personnels et les tendances à l'échelle du Ministère.

3. En partenariat avec le secrétaire ministériel dans ses fonctions de CPRP, la Direction générale de l'innovation, de l'information et de la technologie (DGIIT) devrait veiller à ce que des approches relatives aux EFVP, aux ESA et aux EMR soient mieux harmonisées et intégrées pour permettre d'avoir une vue d'ensemble complète des risques en matière de renseignements personnels et de sécurité (physique et TI) de manière uniforme et en temps opportun.

1.0 Renseignements généraux

1.1 Contexte

Dans le cadre des programmes d'EDSC, il est nécessaire de recueillir, d'utiliser et de divulguer des renseignements personnels détaillés, et parfois de nature délicate. En raison de la portée du mandat d'EDSC, le Ministère détient le plus grand nombre de renseignements personnels du gouvernement fédéral. La protection des renseignements personnels des Canadiens est une priorité du Ministère. C'est pourquoi de nombreuses ressources et une grande attention de la direction ont été accordées à ce sujet.

Le Ministère a été dans le processus de révision de son CGPRP, qui comprenait une initiative de renouvellement pluriannuelle en matière de protection des renseignements personnels. Découlant du plan d'action pour le renouvellement de la protection des renseignements personnels, une version révisée de la PMGRP a été mise en œuvre le 1er avril 2014. La PMGRP et ses directives énoncent l'application de la *Loi sur la protection des renseignements personnels*, L.R.C. (1985), ch. P-21, règlement sur la protection des renseignement personnels, de la *Loi sur le MEDS,*'Code de protection des renseignements personnels[5]', des politiques et des directives du Conseil du Trésor en matière de protection des renseignements personnels et du Code de conduite d'EDSC, de manière à favoriser un régime de politiques robuste pour la protection et l'utilisation judicieuse des renseignements personnels.

La PMGRP s'applique à tous les employés, agents et entrepreneurs d'EDSC ainsi qu'aux entités du portefeuille pour lesquelles le sous-ministre (SM) d'Emploi et Développement social est l'agent comptable désigné. La politique énonce les rôles et les responsabilités de tous les employés, y compris les responsabilités fonctionnelles du secrétariat ministériel, un rôle qui inclut les fonctions de CPRP du Ministère.

Le PRM d'EDSC pour 2014-2015 indique que la protection des renseignements personnels et la sécurité de l'information font partie des cinq principaux risques auxquels le Ministère est exposé. Parmi les principaux facteurs de risque, il y a le volume élevé de renseignements personnels et de nature délicate[6], le grand nombre d'EER, ainsi que les méthodes et les pratiques actuelles de gestion de l'information et de protection des renseignements personnels.

1.2 Objectif de l'audit

L'objectif du présent audit visait à évaluer la pertinence et l'efficacité du CGPRP d'EDSC pour la protection des renseignements personnels des Canadiens.

1.3 Portée

La portée de cet audit s'appliquait aux politiques, processus et pratiques ministériels liés au CGPRP d'EDSC entre avril 2013 et décembre 2014. Plus particulièrement, l'audit a examiné le cadre du point de vue des piliers suivants : gouvernance et responsabilisation; gouvernance des renseignements personnels; culture, formation et sensibilisation; gestion des risques et assurance de la conformité. Ces

---

5 La Partie IV de la législation habilitante, aussi connue sous le nom de Code de protection des renseignements personnels du Ministère, applique au Ministère des règles plus sévères en matière de transmission de renseignements que la *Loi sur la protection des renseignements personnels*, sur laquelle il a préséance.

6 Les renseignements de nature délicate sont des renseignements qui nécessitent une protection supérieure et un devoir de diligence plus rigoureux.

piliers correspondent aux dix principes généralement reconnus en matière de protection des renseignements personnels[7].

1.4 Méthodologie

Un certain nombre de méthodologies ont été utilisées durant la réalisation de l'audit, essentiellement des entrevues avec les principaux membres du régime de protection des renseignements personnels d'EDSC, notamment des membres de la haute direction, des cadres des bureaux régionaux et des programmes, ainsi qu'une revue et une analyse de la documentation.

Le secrétaire ministériel, qui exerce les fonctions de CPRP, était le principal intervenant dans la présente mission. La Direction générale des services d'intégrité, la DGIIT, les Services juridiques ainsi que des directions régionales et des programmes choisis ont également été consultés en vue d'obtenir une vue d'ensemble complète du CGPRP du Ministère.

Même si le présent audit avait pour objectif d'évaluer le CGPRP, il faut noter que d'autres projets d'audit de la version approuvée du Plan de vérification axé sur les risques 2014-2017 examineront en profondeur les diverses composantes du cadre. Ces missions ont été prises en compte par l'équipe d'audit lors de l'établissement de la portée finale de l'audit.

Les travaux de l'audit ont été réalisés entre octobre 2014 et janvier 2015.

2.0 Constatations de l'audit

Pour atteindre les objectifs d'EDSC en matière de protection des renseignements personnels et pour inclure la protection des renseignements personnels dans la conception et l'architecture des programmes, des services, des systèmes et des technologies, le Ministère a mis en place un cadre intégré de gestion de la protection des renseignements personnels fondé sur les piliers suivants :

- **Gouvernance et responsabilisation :** Rôles et responsabilités établis, et mécanismes pour soutenir la conformité du Ministère aux exigences des lois, des règlements, des politiques et des normes et aux attentes du public.

- **Gouvernance des renseignements personnels :** Protection appropriée des renseignements personnels, et ce, tout au long de leur cycle de vie.

- **Culture, formation et sensibilisation :** Une culture respectueuse de la vie privée où les employés, les partenaires et les agents de prestation des services comprennent leurs obligations relativement à la protection de la vie privée et où ils connaissent les outils, les ressources, les politiques et les processus liés à la protection de la vie privée et à la protection des renseignements personnels.

---

6 Établis par l'*American Institute of Chartered Professional Accountants* et l'Institut canadien des comptables agréés en 2009; les principes et les critères figurant dans ce document ont été établis en fonction des exigences réglementaires et des pratiques exemplaires en matière de protection des renseignements personnels à l'échelle internationale. Les dix principes sont les suivants : être responsable, préciser le but de votre démarche, obtenir le consentement, limiter la collecte, limiter l'utilisation, la divulgation et la conservation des renseignements, être exact, prendre des mesures de sécurité adéquates, faire preuve de transparence, donner l'accès aux renseignements personnels et en vérifier la conformité.

- **Gestion des risques :** Efforts délibérés et systématiques pour diminuer la probabilité et l'incidence d'évènements négatifs et pour optimiser les possibilités grâce à la détermination des risques, leur évaluation et l'établissement de priorités.

- **Assurance de la conformité :** Pratiques et processus officiels pour veiller au respect des lois, des politiques et des normes en matière de protection des renseignements personnels.

Les pages qui suivent présentent les points forts et les éléments à améliorer en ce qui a trait au cadre de gestion des renseignements personnels au Ministère :

2.1 Gouvernance et responsabilisation

Des organismes responsables de la gouvernance sont en place et les responsabilités sont définies pour appuyer la gestion et la protection des renseignements personnels

Mise en œuvre en 2014, la PMGRP prévoit que le SM d'Emploi et Développement social est responsable de la conformité du Ministère à l'ensemble des lois et des politiques du Conseil du Trésor concernant la gestion et la protection des renseignements personnels. Cette responsabilité est réaffirmée dans l'*Ordonnance de délégation* du Ministère, signée en août 2010 et actuellement en processus de révision.

La PMGRP définit les rôles et les responsabilités en matière de protection des renseignements personnels, ajoutant que tous les employés sont responsables d'assurer la protection des renseignements personnels sous leur responsabilité et leur contrôle. La PMGRP décrit également les responsabilités fonctionnelles pour les cadres dirigeants qui participent directement à l'administration du cadre, dont le CPRP, l'ASM et le coordonnateur de la sécurité de la TI du Ministère.

Le CPRP détient l'autorité fonctionnelle et agit à titre de conseiller principal du Ministère en ce qui concerne les questions liées à la protection des renseignements personnels, et il est responsable de la conception et de la supervision continues de la PMGRP, de ses directives et instruments connexes, ainsi que du programme de gestion de la protection des renseignements personnels. La description par la PMGRP des rôles fonctionnels du CPRP, de l'ASM et du coordonnateur de la sécurité des TI du Ministère représente un effort important d'intégration des domaines fonctionnels dans la gestion des renseignements personnels.

La PMGRP définit également les comités de surveillance qui appuient la protection des renseignements personnels ainsi que les conséquences découlant des manquements à la politique ou à des lois, des politiques ou des procédures connexes. Le CPRPSI, un sous-comité du Comité de la gestion ministérielle (CGM), est le principal organisme de gouvernance chargé de l'établissement des mandats en matière de protection de la vie privée et de protection des renseignements personnels, y compris l'élaboration de politiques, ainsi que le soutien à la coordination horizontale des questions, des plans et des stratégies et à l'établissement de priorités connexes. Le comité est coprésidé par le CPRP et l'ASM, et il est composé des directeurs généraux des directions générales d'EDSC. Le comité compte également sur une représentation des régions par l'entremise des directeurs exécutifs.

La composition du CPRPSI fournit un point de vue stratégique et horizontal à l'égard des enjeux et des risques en matière de protection des renseignements personnels et ils montrent l'engagement du Ministère à l'égard de l'intégration de la protection des renseignements personnels, de la sécurité des TI et de la GI. Les principales activités du CPRPSI pour 2014 comprenaient la présentation d'orientations sur cinq nouvelles directives en matière de GI-TI afin de répondre au Plan relatif à la sécurité de la GI-TI d'EDSC, la révision du nouveau processus d'ESA, la mise en œuvre d'une nouvelle méthode d'établissement des priorités en matière d'EFVP, l'examen et l'approbation d'un rapport annuel au Parlement sur l'administration de la *Loi sur la protection des renseignements personnels* et l'examen de rapports d'audit externe pertinents portant sur la protection des renseignements personnels.

Le CGM reçoit des mises à jour régulières du CPRPSI relativement aux progrès en matière de protection des renseignements personnels, de la sécurité de la TI, de la sécurité de la GI et de la sécurité physique et il approuve des documents portant sur la protection des renseignements personnels. Parmi les éléments particuliers discutés par le CGM depuis décembre 2013, il y a : examen et approbation des priorités annuelles du CPRPSI, de la directive sur la divulgation de renseignements dans l'intérêt public, de la mise à jour du programme de sécurité de la TI du Ministère, du Plan du secrétariat ministériel et du cadre intégré de sécurité du Ministère. Il a été constaté que de façon générale, les questions touchant la protection des renseignements personnels étaient signalées efficacement au CGM.

Deux des principaux mécanismes utilisés par le Ministère dans son cadre de protection des renseignements personnels sont les EFVP et les EER. Le Secrétariat du Conseil du Trésor exige qu'une EFVP soit effectuée au sujet des programmes ou des initiatives nécessitant l'utilisation ou la communication de renseignements personnels. À EDSC, l'approche du Ministère pour ce qui touche l'élaboration de l'EFVP est perçue comme une pratique exemplaire qui permettra d'assurer que chaque programme ou initiative aura subi une analyse approfondie des risques associés à la protection des renseignements personnels et que des stratégies d'atténuation connexes seront en place avant de pouvoir utiliser des renseignements personnels. Une EER est un protocole d'entente entre EDSC et des tierces parties telles que d'autres ministères fédéraux, des gouvernements provinciaux et des municipalités; l'EER établit les modalités selon lesquelles des renseignements personnels sont partagés entre les parties.

Parmi les activités faisant partie de son mandat, le CPRPSI doit examiner et commenter les EFVP et les EER et recommander leur approbation. L'équipe d'audit a remarqué que les EFVP et les EER étaient des points réguliers à l'ordre du jour qui nécessitaient une grande attention lors des réunions du comité. Le comité est donc considéré par les membres que nous avons interrogés comme étant plutôt axé sur les transactions, se concentrant davantage sur l'examen et l'approbation des EFVP et des EER plutôt que de gérer des questions horizontales élargies associées aux EFVP et aux EER.

Les entrevues avec des cadres des directions régionales et des programmes qui étaient membres du CPRPSI ont permis de constater que l'accent mis sur l'examen et l'approbation des EFVP et des EER a démotivé les membres et les a surchargés de documents. Les membres du comité ne reçoivent souvent les documents relatifs aux EFVP et aux EER qu'un ou deux jours ouvrables avant les réunions, ce qui rend difficile leur examen complet et la formulation de commentaires pertinents. Il est possible d'améliorer le CPRPSI en révisant son approche actuelle afin qu'il puisse gérer les enjeux et les risques horizontaux en matière de protection des renseignements personnels et de sécurité.

2.2 Gouvernance des renseignements personnels

L'accessibilité aux documents pertinents en matière de protection des renseignements personnels a besoin d'amélioration.

La PMGRP permet d'avoir un aperçu du CPRP d'EDSC, qui définit les dix principes en matière de protection des renseignements personnels sur lesquels les politiques, les directives et les procédures connexes sont fondées. La PMGRP est conforme à la *Loi sur le MEDS* (y compris le Code de protection des renseignements personnels que renferme la *Loi sur le MEDS*) et à la *Loi sur la protection des renseignements personnels*, L.R.C. (1985), ch. P-21. EDSC a également mis en œuvre certaines directives en appui à l'ensemble de politiques et à la gouvernance et la protection générales des renseignements personnels.

La Division de la protection des renseignements personnels et le CPRP ont créé une page iService[8] concernant « la gérance des renseignements » dans l'intranet du Ministère pour permettre à l'ensemble des employés d'accéder au cadre ministériel de gestion de la protection des renseignements personnels, notamment des copies des politiques, des directives et autres orientations pertinentes. Il y a également des liens vers de la formation obligatoire et des personnes-ressources pouvant répondre à des questions ou résoudre des problèmes à l'égard de la protection des renseignements personnels.

Malgré tous les efforts du Ministère pour diffuser son ensemble de politiques sur la protection des renseignements personnels, il est difficile de trouver des documents sur la protection des renseignements personnels sur iService et dans l'intranet. L'audit a permis d'observer que la recherche de documents pertinents en matière de protection des renseignements personnels était difficile. Par exemple, trouver la PMGRP au moyen des moteurs de recherche n'a pas été facile. D'autres documents et liens importants étaient désuets.

Il serait souhaitable pour le Ministère qu'il révise son processus de GI, notamment ses conventions d'appellation, l'utilisation de métadonnées[9], le stockage de documents et le téléversement des documents dans l'intranet et d'autres dépôts en temps opportun pour qu'il soit plus facile pour les employés d'EDSC de trouver les politiques et les outils d'orientation liés à la protection des renseignements personnels, à la sécurité, à la TI et à la GI et d'y avoir accès.

La gouvernance des EER demeure un risque

EDSC recueille, utilise et divulgue une quantité substantielle de renseignements personnels pour appuyer la prestation de programmes et services sociaux et relatifs au marché du travail. Il partage également les renseignements personnels de ses clients[10] lorsque la loi lui en donne le pouvoir. Le Ministère gère actuellement plus de 500 ententes connues renfermant des dispositions sur la communication de renseignements avec d'autres institutions fédérales, d'autres paliers de gouvernement, des organisations étrangères et des directions générales et régions d'EDSC. Ces ententes sont appelées EER et elles doivent satisfaire aux exigences de la *Loi sur le MEDS*, à la partie IV (désignée sous le nom de Code de protection des renseignements personnels) et à la *Loi sur la protection des renseignements personnels*, L.R.C. (1985), ch. P-21. La Partie IV exige l'approbation du ministre (ou de son délégué) en ce qui a trait à toute entente écrite avec une organisation à l'extérieur du Ministère dans le cadre de laquelle des renseignements personnels protégés sont partagés. Par l'instrument de délégation de pouvoirs en place depuis 2010, le SM d'EDSC, a été délégué par la Ministre l'autorité de signer des accords qui contiennent des dispositions relatives au partage de l'information. Également, il y a en place un processus exigeant que tous les EER soient examinés par le CPRPSI et recommandés pour la signature du SM. Le risque associé à l'échange de données et des EER repose actuellement sur l'inventaire incomplet des EER conclus par le Ministère.

Dans le PRM 2014-2015, un des principaux facteurs de risques de la « protection des renseignements personnels/sécurité de l'information » était le nombre élevé d'EER qui touchait aux renseignements personnels. Le PRM a établi qu'il était possible que des employés et des tiers[11] aient accès par inadvertance ou de manière inappropriée à des renseignements personnels et de nature délicate d'EDSC et qu'ils recueillent, utilisent, divulguent, conservent et éliminent ces renseignements.

Pour atténuer ce risque, le CGM a approuvé un plan d'action sur les EER en février 2014 afin de répondre aux risques en matière de protection des renseignements personnels et contrôler les écarts. Le plan comprenait une stratégie visant à dresser l'inventaire de l'ensemble des EER, à évaluer ces ententes

---

8 iService fait partie de l'intranet d'ESDC et comprend des renseignements à jour à l'intention des employés sur les services de première ligne des directions générales habilitantes.

9 Les métadonnées définissent d'autres données et facilitent l'identification, la description, la localisation ou l'utilisation des systèmes d'information, des ressources et des éléments conformément aux exigences du Conseil du Trésor.

10 Clients se réfère à des destinataires de services internes et externes.

11 Profil de risque du Ministère 2014–2015, juin 2014, page 11.

pour vérifier leur conformité au Code de protection des renseignements personnels afin d'identifier et de trier les EER qui nécessitent une mise à jour (en utilisant une approche axée sur les risques) et d'établir les priorités qui en découlent.

Il a été observé pendant les travaux de planification de l'audit et au cours de la présente mission que la mise en place d'un dépôt complet comprenant les ententes existantes se faisait toujours attendre. La Division de la protection des renseignements personnels travaille actuellement avec les directions générales et les régions pour établir l'inventaire des EER et faire un tri des risques et aider les directions générales et les régions à comprendre leurs priorités en ce qui a trait aux exigences législatives actuelles. Des efforts constants relativement à l'inventaire des EER sont importants pour aider le Ministère à avoir une idée du nombre d'EER en place.

Recommandation 1

Le Ministère devrait s'assurer que l'inventaire des EER soit terminé en temps opportun et que toutes les ententes renfermant des dispositions relatives à la transmission de renseignements soient définies, évaluées et gérées de manière continue.

Réponse de la direction

Le secrétaire ministériel dans ses fonctions de CPRP et le sous-ministre adjoint principal de la Direction générale des politiques stratégiques et de service sont en accord avec cette recommandation. La Division de la protection des renseignements personnels continuera de gérer les EER jusqu'à ce que le programme de soutien au Chef de la direction de données soit développée à l'automne de 2015.

La surveillance ministérielle des incidents en matière de protection de renseignements personnels et la production de rapports connexes à l'intention du CPRPSI doivent être améliorés

Plusieurs directions générales du Ministère participent à la surveillance des problèmes liés à la protection des renseignements personnels et à la production de rapports à cet égard. La Division de la protection des renseignements personnels, du Secrétariat ministériel, prépare un rapport annuel sur l'administration par EDSC de la *Loi sur la protection des renseignements personnels* pour mettre en lumière les réalisations en matière de gestion de la protection des renseignements personnels, de même que les domaines de préoccupation/amélioration. Le rapport, présenté au Parlement, fournit des statistiques sur les EFVP achevées, les demandes d'information présentées en vertu de la *Loi sur la protection des renseignements personnels*, L.R.C. (1985), ch. P-21, les activités de formation et de sensibilisation relatives à la protection des renseignements personnels, les divulgations dans l'intérêt public, les plaintes et les enquêtes, ainsi que les atteintes importantes à la vie privée.

La DGIIT, chargée de gérer la sécurité de la TI, surveille constamment l'utilisation de dispositifs externes portables non autorisés (p. ex. des dispositifs USB, périphériques de stockage, des disques durs externes). Lorsqu'un incident se produit avec un dispositif portatif non autorisé, la Sécurité de la TI envoie un courriel au gestionnaire de l'employé pour lui expliquer la nature de l'incident. Les courriels envoyés par la Sécurité de la TI concernent des incidents isolés, qui ne sont pas systématiquement signalés aux organismes de gouvernance.

L'ASM collabore avec le CPRP pour tenir à jour la Directive sur la façon d'intervenir en cas d'incidents de sécurité liés à des renseignements personnels et le protocole sur les rapports d'incidents de sécurité du Ministère. L'Unité de gestion des incidents liés à la sécurité (UGIS) de l'ASM a créé des guides de

référence et des outils pour aider les employés en ce qui a trait au signalement des incidents de sécurité. L'UGIS fait un suivi interne pour tous les incidents de sécurité touchant des renseignements personnels en consignant les détails des incidents et les mesures d'atténuation ont été prises.

Même si l'ASM et le CPRP gèrent les incidents liés à la protection des renseignements personnels de façon transactionnelle, davantage d'analyses et de rapports effectués de manière horizontale seraient bénéfiques pour le Ministère. Ces rapports et analyses des tendances réalisés de façon systématique permettraient à l'ASM, au CPRP, à la haute direction et au CPRPSI de prendre des décisions éclairées, stratégiques et horizontales quant à l'orientation du programme de protection des renseignements personnels et de valider les succès ou les lacunes des initiatives mises en œuvre.

Recommandation 2

En partenariat avec le secrétaire ministériel dans ses fonctions de CPRP, l'ASM devrait veiller à la mise en place d'un mécanisme visant à regrouper les rapports sur les incidents liés à la protection des renseignements personnels et les tendances à l'échelle du Ministère.

Réponse de la direction

Le sous-ministre adjoint de la Direction générale des services d'intégrité et le secrétaire ministériel dans ses fonctions de CPRP sont en accord avec la recommandation. La technologie est en cours d'élaboration pour soutenir le rapport des incidents à la vie privée et des tendances à travers le Ministère. Une fois complété en septembre 2015, un rapport trimestriel à l'ASM, le CPRP et le CPRPSI aura lieu.

2.3 Culture, formation et sensibilisation

Des programmes de formation et de sensibilisation ont été mis sur pied

Le Collège Service Canada a mis sur pied le programme de formation obligatoire sur la GICMT qui offre aux employés d'EDSC un aperçu général et intégré du programme ministériel de protection des renseignements personnels, notamment en ce qui a trait à la sécurité de la TI et à la GI. L'objectif de la formation sur la GICMT est de veiller à ce que les employés d'EDSC puissent avoir une compréhension de base de leurs rôles et responsabilités en matière d'utilisation et de gestion de renseignements ministériels et/ou personnels et appliquer correctement les connaissances acquises. Le programme de formation inclut les valeurs et l'éthique, les rôles et les responsabilités associés à la protection des renseignements personnels, les politiques pertinentes, les risques et les menaces, la sécurité ministérielle, la sécurité de la TI, la GI, ainsi que les demandes d'accès à l'information et de protection des renseignements personnels. Le programme traite également des conséquences des manquements aux pratiques prescrites en matière de protection des renseignements personnels.

Après avoir suivi le cours de gestion en ligne, les employés doivent passer un test, remplir un rapport d'apprentissage et passer une évaluation. En date d'août 2014, la formation a été suivie par 98,7 % des employés, qui ont presque tous (99,9 %) passé le test. Le manuel de formation sur la GICMT renvoie vers des documents de référence accessibles dans l'intranet ou sur iService du Ministère.

L'équipe d'audit est d'avis que la formation sur la GICMT est une pratique exemplaire du Ministère, car elle intègre les principes de protection des renseignements personnels aux pratiques de GI-TI.

La haute direction continue d'utiliser de multiples approches pour communiquer l'importance de la gestion et de la protection des renseignements personnels. Parmi les initiatives mentionnées, il y a les séances de sensibilisation conjointes avec le CPRP, l'ASM et le directeur général de la Stratégie, de la planification, de l'architecture et de la gestion de la DGIIT, le site intranet de la gérance de l'information, des vidéos, des courriels des communications ministérielles et les semaines de sensibilisation.

L'audit a toutefois permis d'observer un besoin de renforcement continu des principes liés à la protection des renseignements personnels. Les directions régionales et des programmes ont déclaré que la formation en cette matière était de niveau trop élevé et ne s'appliquait pas vraiment aux employés qui n'étaient pas à l'administration centrale. Une formation mieux adaptée aux employés de première ligne serait plus pertinente pour renforcer les principes de protection des renseignements personnels. Les régions et les programmes ont déclaré que des études de cas et des exemples concrets seraient bénéfique si inclus au programme de formation.

Les entrevues réalisées pendant l'audit ont révélé une « fatigue liée aux communications » au sein du Ministère en raison de la fréquence des communications et du contenu qui ne correspond pas au public cible, en particulier en ce qui concerne les opérations régionales. Enfin, des préoccupations ont été soulevées quant à la question de savoir si les communications étaient réellement comprises par les employés et si les moyens de communication et le renforcement devaient être réévalués.

Il serait avantageux pour la direction de continuer à évaluer l'efficacité de la communication et des stratégies de formation pour s'assurer que le CGPRP est bien compris et appliqué à l'échelle du Ministère. Les approches pourraient inclure la présentation d'études de cas périodiques et le renforcement par les gestionnaires à l'aide de discussions sur les principes de protection des renseignements personnels et leur applicabilité aux employés.

2.4 Gestion des risques

La gestion ministérielle du risque inclut des principes de protection des renseignements personnels, mais les processus de risques relatifs aux EFVP pourraient être renforcés

EDSC dispose de mécanismes pour surveiller les risques liés à la protection des renseignements personnels, notamment le PRM. À l'heure actuelle, la protection des renseignements personnels et la sécurité sont un des principaux risques figurant dans le PRM et dans les registres des risques des directions générales et de programmes. Un des principaux facteurs de risques relatifs à la protection des renseignements personnels et à la sécurité est le nombre élevé d'EER au Ministère. Pour soutenir la compilation du PRM, chaque direction générale fera la compilation des risques propres à ses programmes dans un registre qui sera intégré au PRM. Dans le cadre de ce processus, des entrevues sont réalisées avec des membres de la haute direction, dont ceux du Secrétariat ministériel, afin d'obtenir leur avis sur les risques à l'échelle de l'organisation.

En plus du PRM, le Ministère dispose d'autres processus permettant d'évaluer les risques liés à la gestion et à la protection de renseignements personnels à l'échelle des programmes, y compris des EFVP et des EMR en matière de sécurité de la TI et de sécurité physique.

Conformément à la ligne directrice du Conseil du Trésor, l'objectif clé d'une EFVP consiste à cerner, à communiquer et à atténuer les risques en matière de protection des renseignements personnels qui ne sont pas gérés par l'entremise d'autres mécanismes du Ministère[12]. Il s'agit d'un processus collaboratif qui rassemble une vaste gamme d'ensembles de compétences, dont les risques en matière de protection des renseignements personnels, de sécurité de la TI et de sécurité physique. L'EFVP sert à aider la haute direction à prendre des décisions éclairées en matière de politiques, de conception de systèmes et de passation de marchés.

Au cours de l'audit, l'équipe a révisé six EFVP sur douze qui dataient de décembre 2013 et avaient été présentées au CPRPSI en 2014. L'équipe d'audit a remarqué des incohérences dans la présentation des données sur les risques, notamment : EFVP comprenant un classement complet des risques en matière de protection des renseignements personnels et de sécurité, EFVP soutenues par les EMR sur la sécurité de la TI; et finalement, EFVP comportant des risques considérés comme faibles et des EMR sur la sécurité de la TI incomplètes.

[12] Lignes directrices sur l'évaluation des facteurs relatifs à la vie privée – Cadre de gestion des risques d'entrave à la vie privée, Secretariat du Conseil du trésor du Canada, avril 2012.

Un nouveau processus d'ESA a été proposé en 2014 afin de remplacer les EMR actuelles pour la sécurité de la TI. Le nouveau processus d'ESA devrait permettre d'assurer l'examen et l'atténuation des risques en matière de sécurité de la TI avant que les solutions de TI ne soient mises en œuvre. Il devrait également permettre de surveiller les risques tout au long du cycle de vie de la solution. En outre, le Ministère surveille les risques grâce à la mise en œuvre de PAPRPDP. En 2011, le Ministère a effectué une série d'évaluation des risques des programmes et a élaboré les PAPRPDP en 2012-2013 pour atténuer les risques potentiels cernés en matière de protection des renseignements personnels. Une mise à jour des évaluations des risques est en cours pour cerner et régler plus facilement les problèmes horizontaux entre les programmes.

En 2014, le Ministère a mis en œuvre une nouvelle méthode d'établissement de priorités relatives aux EFVP. La méthode permet de faire le suivi des priorités ministérielles relatives aux EFVP et inclut les niveaux de risques, les contraintes de temps et l'état des EFVP. Cette approche vise à fournir des renseignements utiles aux membres du CPRPSI quant à l'état des EFVP, tout en facilitant l'affectation stratégique des ressources des directions générales habilitantes vers l'élaboration des EFVP prioritaires.

Recommandation 3

En partenariat avec le secrétaire ministériel dans ses fonctions de CPRP, la DGIIT devrait veiller à ce que des approches relatives aux EFVP, aux ESA et aux EMR soient mieux harmonisées et intégrées pour permettre d'avoir une vue d'ensemble complète des risques en matière de renseignements personnels et de sécurité (physique et TI) de manière uniforme et en temps opportun.

Réponse de la direction

Le sous-ministre adjoint de la DGIIT et le secrétaire ministériel dans ses fonctions de CPRP sont en accord avec la recommandation. La technologie est en cours d'élaboration pour soutenir le rapport des incidents à la vie privée et des tendances à travers le Ministère. Une fois complété en septembre 2015, un rapport trimestriel à l'ASM, le CPRP et le CPRPSI aura lieu.

2.5 Assurance de la conformité

Le Ministère utilise divers mécanismes pour surveiller le cadre de gestion des renseignements personnels

Dans l'ensemble, le Ministère a pris diverses approches pour surveiller son cadre de protection des renseignements personnels. Comme nous l'avons mentionné plus tôt dans le présent rapport, une structure de gouvernance spécialisée et fonctionnelle par l'entremise d'organismes tels que le CPRPSI et le CGM, de même que des postes spécialisés tels que le CPRP permettent d'assurer que la protection des renseignements personnels demeure au programme de la direction. En outre, EDSC a également été soumis à des audits internes et externes, qui ont souligné l'existence de points à améliorer. Des plans d'action pour combler les écarts ont été élaborés et leur mise en œuvre est en cours. Enfin, le Bureau des valeurs et de l'éthique prépare des rapports sur les incidents qui touchent le Code de conduite; certains de ces incidents peuvent concerner la protection des renseignements personnels ou la sécurité.

À l'échelle des programmes, les PAPRPDP ont permis de cerner divers secteurs prioritaires courants d'un programme à l'autre. Une mise à jour de l'évaluation des risques est en cours afin de trier les PAPRPDP de façon horizontale et d'en faciliter la surveillance.

Le Ministère surveille les systèmes pour être alerté en cas d'incident ainsi que les contrôles d'accès. Le branchement de clés USB non autorisées sur le réseau à partir de tous les ordinateurs des employés fait l'objet de surveillance. La DGIIT a également effectué un balayage des courriels sortants et d'attaques d'hameçonnage. L'ASM a mis en place des ratissages de sécurité à l'AC; de plus, l'équipe d'audit a été informée que des ratissages de sécurité seront mis en place dans les régions en 2015-2016. En ce qui a trait aux contrôles d'accès, les directions des programmes ont affirmé lors des entrevues qu'il était possible de renforcer le contrôle des accès des employés aux divers systèmes. Ils ont donné l'exemple d'employés qui ont quitté le Ministère ou qui ont été mutés dans un autre secteur d'EDSC sans que leurs droits d'accès ne soient révoqués. Des lacunes en ce qui concerne la surveillance de l'accès ont été soulevées lors des audits précédents. Des plans d'action ont été élaborés et sont actuellement mis en œuvre pour combler les écarts qui ont été cernés.

3.0 Conclusion

L'audit a permis de constater que le CGPRP d'EDSC permet de répondre adéquatement à la plupart des questions touchant la protection des renseignements personnels. Des processus et des contrôles durables sont en place, notamment un organisme de gouvernance spécial et un ensemble de politiques en matière de gestion des renseignements personnels. Cependant, certains domaines du CGPRP peuvent encore être améliorés. Il est possible de mieux intégrer les processus de l'EFVP, de l'ESA et de l'EMR pour la production de rapports consolidés sur les tendances en matière d'incidents liés aux renseignements personnels et pour améliorer la gestion des EER.

4.0 Énoncé d'assurance

Selon notre jugement professionnel, les procédures d'audit appliquées et les éléments probants recueillis sont suffisants et appropriés pour confirmer l'exactitude des conclusions présentées dans ce rapport. Les conclusions ont été fondées sur une observation et une analyse des situations qui existaient au moment de l'audit. Les éléments probants ont été recueillis conformément aux Normes relatives à la vérification interne au sein du gouvernement du Canada et aux Normes internationales pour la pratique professionnelle de l'audit interne.

Annexe A : Évaluation des critères d'audit

Élément de contrôle	Critères Il est attendu que :	Cote
Gouvernance et responsabilisation	La structure de gouvernance d'EDSC traite clairement de la gestion de la protection des renseignements personnels.	●
	EDSC définit, consigne, communique et assigne les responsabilités à l'égard de ses politiques et de ses procédures en matière de protection des renseignements personnels.	●
	Les politiques et les procédures en matière de protection des renseignements personnels sont examinées et comparées aux exigences des lois et des règlements applicables.	✪
Gouvernance des renseignements personnels	Le cadre de contrôle visant à protéger les renseignements personnels tout au long du cycle de vie de l'information est défini, consigné et respecte la *Loi sur la protection des renseignements personnels*, L.R.C. (1985), ch. P-21 et la *Loi sur le MEDS*.	●
	Les politiques en matière de protection des renseignements personnels et les conséquences de ne pas s'y conformer sont diffusées aux membres du personnel d'EDSC responsables de la collecte, de l'utilisation, de la conservation et de la divulgation des renseignements personnels.	●
	Les types de renseignements personnels et de nature délicate et les processus connexes, les systèmes et les tiers participant au traitement de tels renseignements sont cernés. Ces données sont traitées dans les politiques et les procédures d'EDSC en matière de protection des renseignements personnels ainsi que dans les politiques et les procédures connexes en matière de sécurité.	⭘
	Un programme documenté de gestion des atteintes à la vie privée et des incidents liés aux renseignements personnels a été mis en œuvre.	⭘
Culture, sensibilisation et formation	Un programme de sensibilisation à la protection des renseignements personnels est en place, et une formation est offerte à certains membres du personnel en fonction de leur rôle et de leurs responsabilités.	●
	Le Ministère dispose d'un Code de conduite qui traite des attentes en matière de protection des renseignements personnels.	●
Gestion des risques	Un processus d'évaluation des risques sert à établir des points de référence pour les risques, à cerner et à évaluer les risques nouveaux ou modifiés à l'égard des renseignements personnels ainsi qu'à concevoir et à mettre à jour des réponses à ce chapitre.	⭘
	La direction mesure son rendement par rapport aux attentes définies sur le plan de la gestion de la protection des renseignements personnels et en fait rapport.	●

Élément de contrôle	Critères Il est attendu que :	Cote
Assurance de la conformité	Le Ministère surveille la conformité à ses politiques et à ses procédures de protection des renseignements personnels et met en place des procédures pour répondre aux demandes de renseignements, aux plaintes et aux différends en matière de protection des renseignements personnels.	●

✪ = Pratique exemplaire
● = Les contrôles sont suffisants, exposition faible au risque
◉ = Les contrôles ont été effectués, mais ils pourraient être renforcés; exposition modérée au risque
○ = Absence de contrôles clés, exposition élevée au risque

Annexe B : Glossaire

ASM	Agent de sécurité du Ministère
CGM	Comité de la gestion ministérielle
CGPRP	Cadre de gestion de la protection des renseignements personnels
CPRPSI	Comité de la protection des renseignements personnels et la sécurité de l'information
CPRP	Chef de la protection des renseignements personnels
CPVP	Commissariat à la protection de la vie privée
DGIIT	Direction générale de l'innovation, de l'information et de la technologie
EDSC	Emploi et Développement social Canada
EER	Entente sur l'échange de renseignements
EFVP	Évaluation des facteurs relatifs à la vie privée
EMR	Évaluation des menaces et des risques
ESA	Évaluation de la sécurité et de l'autorisation
GI	Gestion de l'information
GICMT	Gestion de l'information et comportements en milieu de travail
MEDS	Ministère de l'Emploi et du Développement social
PAPRPDP	Plans d'action en matière de protection des renseignements personnels dirigés par les programmes
PMGRP	Politique ministérielle sur la gestion des renseignements personnels
PRM	Profil de risque du ministère
SM	Sous-ministre
TI	Technologie de l'information
UGIS	Unité de gestion des incidents liés à la sécurité