Veterans Affairs Canada | Anciens Combattants Canada

Évaluation des risques liés à la gestion de l'information

Version finale - Août 2011

Canada

REMERCIEMENTS

L’équipe chargée de l’examen tient à remercier tous ceux qui ont aidé à l’évaluation. Elle reconnaît en particulier l’assistance et la coopération de la direction et des employés d’Anciens Combattants Canada de la Direction générale de la technologie de l'information et de la gestion de l'information concernés par la présente évaluation des risques.

TABLE DES MATIÈRES

SOMMAIRE i
1.0 CONTEXTE 1
2.0 INFORMATION SUR L'ÉVALUATION DES RISQUES 6
2.1 Objectifs 6
2.2 Portée 6
2.3 Méthode 7
3.0 SOMMAIRE DE L'ÉVALUATION DES RISQUES 8
3.1 Entités à risque élevé 9
3.1.1 Planification de la continuité des activités (y compris le plan de continuité des activités de la TI) 9
3.1.2 Demandes relatives à l'accès à l'information et à la protection des renseignements personnels (AIPRP) 11
3.1.3 Évaluation des facteurs relatifs à la vie privée 13
3.1.4 Accès à l'information et protection des renseignements personnels 14
3.2 Entités à risque moyen 15
3.2.1 Politiques relatives à la sécurité de la TI 15
3.2.2 Fonds de renseignements 16
3.2.3 Plan de continuité de la GI 17
3.2.4 Évaluations de la menace et des risques 18
3.3 Entités à risque faible 18
3.3.1 Gestion des formulaires 18
3.3.2 Conseils et orientation 19
3.3.3 Surveillance et prévention des pourriels 19
3.3.4 Conditions relatives à la GI dans les énoncés de travaux (EDT) et les contrats 20
3.3.5 Révision et traduction 20
3.3.6 Bibliothèque 21
4.0 Conclusion 22
5.0 Distribution 24
Appendice 1 : ANALYSE DE L'EXPOSITION AU RISQUE – CLASSEMENT PONDÉRÉ 25

SOMMAIRE

L'information constitue un bien organisationnel vital qui permet au gouvernement d'offrir des programmes et des services au public, de prendre des décisions éclairées et de favoriser la transparence et la reddition de comptes à l'échelle du gouvernement. La gestion de l'information a pour objectif d'acheminer l'information voulue aux bonnes personnes, au bon endroit et au bon moment.

Sous réserve des exceptions prévues au paragraphe 8(2), la *Loi sur la protection des renseignements personnels* exige que les renseignements personnels ne servent qu'aux fins pour lesquels ils ont été recueillis et qu'ils soient communiqués avec le consentement de la personne concernée qu'en cas de besoin de savoir seulement. À l'automne 2010, le Commissariat à la protection de la vie privée du Canada a enquêté sur une plainte prétendant qu'Anciens Combattants Canada avait fait une grave erreur dans le traitement des renseignements personnels d'une personne. Le Commissariat à la protection de la vie privée a conclu que le Ministère ne respectait pas la loi fédérale relative à la vie privée et a demandé la mise en place de contrôles améliorés afin de protéger l'information délicate contre la diffusion généralisée au sein du Ministère. Ce dernier a élaboré un plan d'action en 10 points en réponse aux recommandations de la commissaire à la protection de la vie privée. Le plan d'action surpasse grandement les recommandations formulées dans le rapport, consolidant ainsi la protection des renseignements personnels et la capacité du personnel d'offrir des services de qualité.

En janvier 2011, la Direction générale de la vérification et de l'évaluation a entrepris l'évaluation des risques liés à la gestion de l'information au sein du Ministère. L'évaluation des risques visait à fournir à la haute direction une analyse détaillée de tous les volets de la gestion de l'information au Ministère pour garantir qu'Anciens Combattants Canada a pris les mesures nécessaires en vue de tous les risques éventuels. Au total, 14 entités concernées par la gestion de l'information ont été analysées au moyen d'une méthode d'analyse du risque élaborée par le Bureau du contrôleur général.

Les résultats de l'analyse du risque des 14 entités (quatre à risque élevé, quatre à risque moyen et six à risque faible) confirment que le Ministère a accompli d'importants progrès depuis l'automne 2010. Cependant, compte tenu de l'importance de la gestion de l'information et de la sensibilité actuelle, même à la lumière des progrès, quatre entités (planification de la continuité des activités, accès à l'information et demandes de renseignements personnels, évaluations des facteurs relatifs à la vie privée, et accès à l'information et protection des renseignements personnels) sont jugées comme étant à risque élevé, et les points suivants doivent faire l'objet de l'attention de la direction :

- L’absence d’un plan de continuité des activités de la TI éprouvé et entièrement fonctionnel expose le Ministère à un risque notable et pourrait mener à l’interruption de la prestation des services du Ministère.

- L’absence d’un centre désigné des activités d’urgence expose le Ministère au risque dans l’éventualité d’un incident majeur.

- Le développement d’un système de gestion des documents et dossiers électroniques a été approuvé en principe, mais les fonds n’ont pas été obtenus. L’absence actuelle d’un tel système rend la saisie et la réception de l’information problématiques.

- Anciens Combattants Canada ne respecte pas le délai d’exécution de 30 jours pour les demandes relatives à l'accès à l'information et à la protection des renseignements personnels (AIPRP), ce qui va à l’encontre de la *Loi sur l'accès à l'information.*

- Le plan actuel de continuité de la gestion de l'information (GI) n’est pas suffisamment précis quand aux rôles, aux responsabilités et à l’obligation de rendre compte. Le processus d’envoi de l’information à Matane (Québec) et de retour de cette information accroît le risque de perte de l’information ou de son égarement, amplifiant l’importance d’un plan de continuité de la GI bien établi.

- La transformation a pour objectif la refonte de la prestation des services et la réduction de la complexité des programmes, d’où le besoin de mener des évaluations additionnelles des facteurs relatifs à la vie privée. Cela aura pour conséquence d’accroître la charge de travail et possiblement d’altérer les responsabilités.

Recommandation		
Il est recommandé au sous-ministre adjoint, Services ministériels, de présenter les risques susmentionnés au Comité de la haute direction pour déterminer l'approche que le Ministère adoptera pour gérer ces risques.		
Mesure corrective à prendre	**Bureau de première responsabilité**	**Date cible**
Première séance d'information sur la GI – Le point	GITI	Juin 2011
Séance d'information au CHD – Évaluation des risques liés à la GI	V et É, SMA des SM	Juillet 2011
Mise à jour de la stratégie de la GI et élaboration du plan de mise en œuvre	GITI	Septembre 2011
Mise en œuvre du plan en parallèle au programme de transformation	GITI	Mars 2014

L'original a été signée par *27 juillet 2011*

_____ _____

Don Love
Dirigeant principal de la vérification

Date

Les membres de l'équipe chargée de l'examen étaient :

Jonathan Adams, directeur, Direction générale de la vérification et de l'évaluation
Roger Doiron, directeur de la vérification
Tim Brown, agent de vérification et d'évaluation
Sivajan Nagulesapillai, aide vérificateur

1.0 CONTEXTE

L'information constitue un bien organisationnel vital qui permet au Ministère d'offrir des programmes et des services au public, de prendre des décisions éclairées et de favoriser la transparence et la reddition de comptes à l'échelle du gouvernement. La gestion de l'information a pour objectif d'acheminer l'information voulue aux bonnes personnes, au bon endroit et au bon moment.

Les Canadiens ont besoin d'avoir accès à un vaste éventail de renseignements sur le gouvernement. Le public s'intéresse vivement à la transparence, voulant s'assurer que le gouvernement rend compte de ses objectifs et que les résultats peuvent être mesurés en fonction de ces objectifs. Du coup, cela rend le gouvernement plus responsable à l'égard des électeurs et facilite la participation informée du public à l'élaboration des politiques d'intérêt public.

À l'été 2010, une plainte a été déposée devant la commissaire à la protection de la vie privée du Canada au sujet de la façon dont Anciens Combattants Canada a géré les renseignements personnels d'une personne. La commissaire à la protection de la vie privée du Canada est un ombudsman spécial qui a le pouvoir d'enquêter sur les plaintes concernant la protection de la vie privée présentées par des citoyens canadiens contre le gouvernement du Canada pour infraction à la *Loi sur la protection des renseignements personnels* concernant les renseignements personnels de particuliers. À l'automne 2010, le Commissariat à la protection de la vie privée du Canada a achevé une enquête et a déterminé certaines circonstances où ACC a enfreint à la *Loi sur la protection des renseignements personnels* dans sa façon de traiter les renseignements personnels.

Sous réserve des exceptions prévues au paragraphe 8(2), la *Loi sur la protection des renseignements personnels* exige que les renseignements personnels ne servent qu'aux fins pour lesquelles ils ont été recueillis et qu'ils soient communiqués avec le consentement de la personne concernée qu'en cas de besoin de savoir seulement. La commissaire à la protection de la vie privée a conclu à l'insuffisance des mesures de protection des renseignements personnels contre la diffusion généralisée au sein du Ministère et a formulé les recommandations suivantes :

- Entreprendre immédiatement l'élaboration d'un cadre amélioré de protection des renseignements personnels comprenant des mesures de protection et des contrôles adéquats visant à restreindre l'accès aux renseignements personnels au sein du Ministère;

- Revoir les politiques et les pratiques de gestion de l'information en place afin de s'assurer que les renseignements personnels ne sont communiqués qu'aux employés du Ministère qui en ont besoin;

- Transmettre à tous les employés le cadre resserré de politique en matière de protection des renseignements personnels. Offrir aux employés une formation sur le traitement approprié des renseignements personnels.

Un plan d'action en 10 points portant sur la protection des renseignements personnels a été élaboré en réponse aux recommandations de la commissaire à la protection de la vie privée. Le plan d'action dépasse de loin les recommandations du rapport, resserre la protection des renseignements personnels et apporte d'importantes améliorations au cadre de gestion de la protection de la vie privée d'ACC. Tous les employés d'ACC sont responsables de la gestion de l'information. La GI dépasse largement les limites de la Direction des services de gestion de l'information (DSGI), et l'accent additionnel qui sera mis sur la GI mènera à une modification majeure de la culture d'ACC.

Voici la liste des 10 points du plan d'action du ministre accompagnés de leur situation actuelle.

Point du plan d'action	**Situation actuelle**
1. Examiner en détail l'accès aux systèmes Examen détaillé d'environ 2 800 comptes d'utilisateurs du Réseau de prestation des services à la clientèle (RPSC).	L'unité de la sécurité de la technologie de l'information surveille maintenant les rapports d'activités, examine l'accès au système électronique du RPSC et enquête s'il y a lieu.
2. Communiquer la politique en matière de discipline Une politique et des lignes directrices renforcées en matière de discipline ont été rédigées et communiquées au personnel.	Un courriel a été envoyé à tous les employés du Ministère le 4 janvier 2011 informant sur le processus continu de surveillance de l'accès au RPSC et des mesures disciplinaires qui seront prises au besoin.
3. Introduire une étape de protection de la vie privée dans la démarche de rédaction des notes d'information De nouvelles procédures ont été communiquées concernant l'utilisation appropriée des renseignements des anciens combattants aux fins de la préparation de notes d'information et d'autres documents utilisés au Ministère.	Les Lignes directrices sur le traitement des renseignements personnels dans la préparation de documents d'information d'ACC ont été communiquées à l'échelle du Ministère de sorte que les notes d'information à la haute direction ne contiennent que l'information requise.

Point du plan d'action	Situation actuelle
4. Nommer un expert en systèmes externe Des experts externes en gestion des systèmes d'information électronique vont examiner les systèmes du Ministère et formuler des recommandations.	Un expert externe en systèmes informatique de CANAFE a examiné les systèmes d'ACC et a produit un rapport comprenant des recommandations.
5. Nommer un expert externe en protection de la vie privée Une équipe d'experts en matière de gestion de renseignements gouvernementaux et de protection des renseignements personnels travaille avec le gouvernement. Ces experts examineront les pratiques ayant cours au Ministère et recommanderont des changements à apporter aux processus afin de s'assurer que les renseignements sont protégés et que leur accès est contrôlé.	Entre octobre et décembre 2010, un expert en protection de la vie privée du SCT a aidé ACC à faire l'examen des politiques et des procédures pour le nouveau cadre de protection de la vie privée. La nouvelle infrastructure de protection des renseignements personnels a été élaborée en février 2011 pour présenter le comité directeur de la protection des renseignements personnels, le chef de la protection des renseignements personnels et le coordonnateur de l'AIPRP.
6. Améliorer la surveillance des systèmes électroniques Une équipe s'affaire à surveiller et à examiner qui a accès à l'information et enquête au besoin. Dans l'éventualité d'un accès inapproprié, des mesures disciplinaires seront prises.	Depuis octobre 2010, l'unité de la sécurité de la TI surveille les rapports d'activités, fait l'examen de l'accès au RPSC et fait enquête au besoin. Un courriel a été envoyé à tous les employés du Ministère le 4 janvier 2011 informant sur le processus continu de surveillance de l'accès au RPSC et des mesures disciplinaires qui seront prises au besoin.
7. Fournir une formation obligatoire en matière de protection des renseignements personnels Un programme de formation obligatoire à l'intention de l'ensemble du personnel a débuté le 19 octobre 2010. On y aborde le « besoin de savoir », la nécessité d'obtenir le consentement de l'ancien combattant	Des séances de sensibilisation au « besoin de savoir » obligatoires pour tout le personnel ont été organisées (environ 82 % des employés ont suivi la formation jusqu'à maintenant). De plus, l'information sur le « besoin de savoir » fait maintenant partie du programme de cours « La gestion de

Point du plan d'action	Situation actuelle
lorsqu'on échange des renseignements et la gamme des mesures disciplinaires qui seront prises en cas d'atteinte à la vie privée. L'Hôpital Sainte-Anne, hôpital agréé, a ses propres programmes en matière de protection de la vie privée et de confidentialité des renseignements sur les anciens combattants.	l'information au travail – GI démystifiée » et des séances d'orientation pour les gestionnaires. En outre, depuis juin 2011, les séances sur le « besoin de savoir » sont également offertes aux étudiants et aux nouveaux employés du Ministère.
8. Fournir une formation approfondie sur les politiques et procédures du gouvernement en matière de protection de la vie privée Une formation approfondie sera donnée à tous les employés sur les nouvelles politiques, lignes directrices et procédures.	En mars 2011, des séances de formation approfondie et des discussions ont pris place avec les équipes de gestion de toutes les directions générales du Ministère, y compris les bureaux régionaux. On a alors expliqué en détail le cadre, les politiques et les lignes directrices relatifs à la gestion de la protection de la vie privée.
9. Effectuer une évaluation indépendante annuelle Une évaluation indépendante sur la conformité par ACC à la *Loi sur la protection des renseignements personnels* et à la *Loi sur l'accès à l'information* sera effectuée tous les ans.	En juillet 2011, Services de vérification Canada de Travaux publics et Services gouvernementaux Canada ont achevé une évaluation indépendante de la conformité du Ministère à la *Loi sur l'accès à l'information* et à la *Loi sur la protection des renseignements personnels*. L'évaluation visait à déterminer si les politiques et les procédures étaient rédigées de sorte que les services soient offerts dans le respect des deux lois.
10. Se préparer pour la vérification de la commissaire à la protection de la vie privée Le Ministère a commencé à se préparer pour la vérification en profondeur que la commissaire à la protection de la vie privée commencera immédiatement.	Le Ministère a entrepris de nombreuses initiatives continues, comme les 10 points du présent plan d'action, en préparation de la vérification de la commissaire à la protection de la vie privée qui aura lieu à l'automne 2011.

Trois initiatives distinctes ont été élaborées à l'appui du plan d'action susmentionné. La première concerne l'évaluation des risques liés à la gestion de l'information au sein d'ACC pour s'assurer que le Ministère a répondu adéquatement à tous les risques éventuels. La seconde est une évaluation externe menée par Services de vérification Canada de la conformité d'ACC à la *Loi sur la protection des renseignements personnels* et à la *Loi sur l'accès à l'information*, ce qui constitue le neuvième point du plan d'action en 10 points portant sur la protection des renseignements personnels. L'évaluation externe sera achevée en juillet 2011. La troisième initiative est la vérification, par le Commissariat, de l'accès à l'information et de la protection des renseignements personnels à ACC qui doit débuter à l'automne 2011.

2.0 INFORMATION SUR L'ÉVALUATION DES RISQUES

2.1 Objectifs

Avant l'enquête du Commissariat à la protection de la vie privée (le Commissariat), la Direction générale de la vérification et de l'évaluation avait déterminé le besoin d'une vérification de la gestion de l'information dans le cadre du plan de vérification 2010-2013. Le début de la vérification avait d'abord été prévu pour l'automne 2010; cependant, en raison de l'enquête du Commissariat, il a été décidé de la reporter pour pouvoir tenir compte des résultats de l'enquête du Commissariat dans la détermination de la portée de la vérification. En janvier 2011, il a été convenu qu'une évaluation des risques liés à la gestion de l'information au sein du Ministère serait plus profitable à la haute direction qu'une vérification. L'évaluation des risques visait à fournir à la haute direction une analyse détaillée de tous les aspects de la gestion de l'information au sein du Ministère pour s'assurer qu'ACC a répondu de façon adéquate à tous les risques éventuels. L'évaluation des risques liés à la GI a pour objectif d'évaluer les principales unités concernées par la GI à ACC.

Le risque est défini dans le cadre international de référence des pratiques professionnelles de l'Institut des vérificateurs internes comme étant la « possibilité qu'un événement ait lieu qui aura une incidence sur l'atteinte des objectifs » et il « est mesuré en fonction des répercussions et des probabilités » [traduction libre].

Dans le document sur les normes de rendement 2120 en gestion du risque (Performance Standard 2120: Risk Management), le cadre de référence précise que la fonction de vérification interne doit comprendre l'évaluation de l'efficacité et contribuer à l'amélioration des processus de gestion du risque.

2.2 Portée

La portée de l'évaluation des risques incluait l'univers entier de la GI à ACC. L'évaluation touchait également toutes les politiques et pratiques en vigueur le 1er avril 2011 et tenait compte des progrès accomplis depuis l'automne 2011 et des travaux prévus.

Il est important de souligner que l'univers de la GI à ACC ne concerne pas uniquement la Direction des services de gestion de l'information (DSGI). L'équipe chargée de l'examen s'est également intéressée aux entités de la Direction de la sécurité et des services immobiliers et de la Direction de l'infrastructure de la TI et des opérations.

2.3 Méthode

L'évaluation des risques a été menée conformément aux Normes internationales pour la pratique professionnelle de la vérification interne de l'Institut des vérificateurs internes, comme l'exige le Conseil du Trésor dans sa Politique sur la vérification interne.

L'évaluation de l'exposition au risque des entités examinées a été menée, conformément au Guide de planification de la vérification interne des ministères et des organismes produit par le Secteur de la vérification du Bureau du contrôleur général du Canada. La méthode comprenait la classification des entités vérifiées en fonction d'une série de critères d'établissement des priorités. L'équipe chargée de l'examen a appliqué les critères à chacune des entités selon l'information recueillie au cours de l'examen des documents, des entrevues et de la consultation avec la haute direction.

L'analyse de l'exposition au risque a été faite en examinant les considérations liées au risque, les événements à risque éventuel et les événements récents pour chacun des cinq principaux facteurs de risque – niveau et nouveauté du changement, niveau de complexité, exigences prévues par la loi ou autres exigences de conformité, niveau de connaissances et niveau de dépendance – pour chaque entité vérifiable. Les niveaux de risque ont été calculés en donnant une cote à la probabilité et à l'incidence de chacun des principaux facteurs de risque. La somme des niveaux de risque pour chaque principal facteur de risque a été multipliée par une signification pour déterminer le risque pondéré de chaque entité.

L'équipe chargée de l'examen a d'abord déterminé 27 entités vérifiables au sein de l'univers de la GI à ACC. Ces entités ont ensuite été combinées par l'équipe chargée de l'examen puisque plusieurs d'entre elles avaient des fonctions et des qualités semblables.

L'appendice 1 (Analyse de l'exposition au risque – Classement pondéré) est un tableau de priorité des entités classées selon une cote pondérée. La cote la plus élevée possible des risques évalués est de 90, et la note la plus faible des risques évalués est de 10. Il faut souligner que l'équipe a appliqué une méthode d'analyse, de prévision rationnelle et de la preuve pour déterminer la pondération aux fins de l'évaluation des risques.

3.0 SOMMAIRE DE L'ÉVALUATION DES RISQUES

Le tableau suivant illustre le classement des entités évaluées par l'équipe chargée de l'évaluation selon une pondération éle3vée, moyenne ou faible. Consulter l'appendice 1 (Analyse de l'exposition au risque – Classement pondéré) pour plus de détails.

INCIDENCE			
ÉLEVÉE		Évaluations des facteurs relatifs à la vie privée	Plan de continuité des activités Demandes relatives à l'AIPRP Accès à l'information et à la protection des renseignements personnels
MOYENNE		Politiques relatives à la sécurité de la TI Fonds de renseignements Plan de continuité de la GI Évaluations de la menace et des risques	
FAIBLE	Gestion des formulaires Conseils et orientation Surveillance et prévention des pourriels Conditions relatives à la GI dans les EDT et les contrats Révision et traduction Bibliothèque		
	FAIBLE	MOYENNE	ÉLEVÉE
		PROBABILITÉ	

3.1 Entités à risque élevé

3.1.1 Planification de la continuité des activités (y compris le plan de continuité des activités de la TI) (90)

La Politique sur la sécurité du gouvernement et les normes qui l'accompagnent décrivent les exigences fondamentales en matière de sécurité, y compris l'établissement d'un programme de planification de la continuité des activités. La planification de la continuité des activités permet aux organismes de survivre pendant les interruptions tout en continuant d'offrir les programmes et les services essentiels et elle est la pierre d'assise de la sécurité ministérielle et de l'état de préparation aux situations d'urgence. Les plans de continuité des activités prévoient également une structure de régie, les chaînes de commandement, l'obligation de rendre compte et la responsabilité relative aux activités jugées essentielles. Le plan doit également préciser les stratégies de communication en situation d'urgence, les plans de formation et les options de rétablissement et établir des dispositions pour l'essai, la vérification et l'examen continus du plan. L'absence d'un plan de continuité des activités pourrait probablement entraîner d'importants inconvénients pour les Canadiens et le gouvernement en cas d'interruption. Le Comité de la haute direction d'ACC est la compétence désignée pour appuyer le programme de planification de la continuité des activités.

Les plans de continuité des activités de chaque secteur seront modifiés étant donné qu'ACC œuvre actuellement à la révision de nombre de ses programmes et activités en raison de la transformation. Le Ministère se prépare également au départ à la retraite de nombreux employés au cours des cinq prochaines années, et la perte conséquente du savoir ministériel et des compétences exposera le Ministère à un risque accru. La planification de la continuité des activités comprend un processus exhaustif de formation et de certification. De plus, les ministères doivent dépendre de chacune de leurs unités pour l'élaboration de leur plan respectif de continuité des activités fiable et pouvant être mis en œuvre. Le niveau de codépendance est élevé avec les autres ministères et établissements étant donné qu'ils seraient appelés à aider. Tous les secteurs d'ACC ont leur propre plan de continuité des activités, à l'exception d'une seule.

Le plan de continuité de la TI est une des principales composantes d'un plan de continuité des activités. Un plan de continuité de la TI fait en sorte que les services de la TI qui sont considérés comme essentiels seront disponibles selon un délai de rétablissement préapprouvé. La planification de la continuité des activités consiste en l'élaboration de plans, de procédures et de dispositions garantissant peu ou pas d'interruption à la disponibilité des biens et des services de TI essentiels. Le plan de continuité des activités de la TI est une composante fondamentale visant à garantir que

l'information est disponible pour la poursuite de la prestation des services. La majorité des directions générales et des directions d'ACC ont leur propre plan de continuité des activités, qui comprend des éléments de la continuité des activités de la TI. Cependant, l'absence d'un plan de continuité de la TI complet et éprouvé pour le Ministère menace la viabilité de divers plans de continuité ministériels et contrevient également à la *Politique sur la sécurité du gouvernement*. L'absence d'un plan de continuité de la TI solide et éprouvé aura un effet général négatif sur l'exécution du plan de continuité des activités.

Le Ministère sera fortement dépendant d'un plan de continuité de la TI dans l'éventualité d'un incident majeur étant donné que le plan précise les rôles, les responsabilités et l'obligation de rendre compte du personnel en plus du lieu de l'équipement de réserve ou de remplacement. Le plan permettra également d'harmoniser les biens et les services technologiques entre l'Administration centrale, les régions et les bureaux locaux à la grandeur du pays. La complexité d'harmoniser le personnel et la dépendance à l'égard de la disponibilité de l'équipement et du personnel à l'échelle du pays dans l'éventualité d'un désastre majeur ne peut être soulignée suffisamment. L'exécution du plan de continuité des activités dépend essentiellement de l'existence d'un centre des activités d'urgence. Vu la fréquence accrue des épidémies, des désastres, des menaces liées à la TI, etc., il existe un risque permanent de perturbation massive des activités. Qu'il s'agisse de la technologie de l'information ou des ressources humaines, il y aura des problèmes non anticipés. Si le Ministère n'est pas préparé, il faudra voir à atténuer l'anxiété, la confusion et la peur des employés. L'ébauche d'un mandat daté du 1er avril 2011 a été rédigée précisant les responsabilités désignées d'un centre des activités d'urgence possédant les ressources voulues pour répondre efficacement et avec efficience en cas de crise. Le centre n'a ni été approuvé ni intégré au plan de continuité des activités.

L'absence d'un plan de continuité de la TI accroît également les risques d'échec éventuel de la mise en œuvre du programme de transformation, de préjudice à la santé et aux finances des anciens combattants, et de perte éventuelle de l'information sur les anciens combattants, et l'attention médiatiques défavorables qui les accompagnera. Le risque le plus important est une interruption éventuelle catastrophique de toutes les activités ministérielles en raison de l'absence d'un plan de continuité des services. De plus, des cyberattaques récentes survenues en 2010-2011 sur les ministères du gouvernement fédéral comme le ministère des Finances augmente le besoin d'un plan de continuité de la TI entièrement financé et éprouvé.

En février 2009, ACC a élaboré et approuvé en principe un plan de continuité de la TI; le plan n'a cependant pas été mis en œuvre par manque de ressources. Depuis 2009, les secteurs des activités d'ACC et l'environnement de la TI ont changé de façon notable en réponse aux nouvelles technologies et aux menaces, rendant ainsi le plan éventuellement périmé. Dans le cas d'un des principaux systèmes, le Système fédéral de

traitement des demandes de soins de santé (SFTDSS), un plan de continuité de la TI éprouvé est en place. Ce plan de continuité de la TI a été élaboré et est géré par un entrepreneur externe et il était une des principales exigences du contrat. Malheureusement, dans le cas des autres systèmes d'ACC, comme le Réseau de prestation des services aux clients (RPSC) et FreeBalance, qui contient la majorité de l'information ministérielle et gouvernementale, il n'existe aucun plan de continuité de la TI, ce qui va à l'encontre de la *Politique sur la sécurité du gouvernement*.

Avant la présente évaluation, la Direction générale de la vérification et de l'évaluation avait prévu exécuter la vérification du plan de continuité de la TI d'ACC en 2011-2012. Vu l'absence d'un tel plan et les préoccupations plus générales concernant le domaine de la gestion de l'information, la présente évaluation des risques a été exécutée au lieu d'une vérification.

3.1.2 Demandes relatives à l'accès à l'information et à la protection des renseignements personnels (AIPRP) (78)

L'Unité de l'AIPRP de la DSGI traite directement avec les employés et le public pour répondre à des demandes officielles et non officielles relativement aux dossiers qui peuvent être communiqués en vertu de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*. L'Unité sert de centre d'expertise pour toutes les questions touchant l'AIPRP. Toutes les directions générales à l'Administration centrale et toutes les régions ont à leurs services un agent de liaison de l'AIPRP chargé de la coordination des demandes de renseignements.

La *Loi sur l'accès à l'information* accorde au public le droit d'accès, sous réserve de certaines exceptions, à la vaste majorité des dossiers qui appuient la gestion et l'exécution des programmes et des activités du gouvernement fédéral. La *Loi sur la protection des renseignements personnels* protège la vie privée des particuliers par la protection de leurs renseignements personnels et accorde aux particuliers le droit d'accès à leurs propres renseignements personnels. Lorsque l'accès est demandé en vertu de ces lois, ACC doit indiquer au demandeur si l'accès au dossier sera ou non accordé dans les trente jours suivant la demande. En 2010-2011, 488 demandes officielles ont été présentées, ce qui représente une augmentation de 57 % comparativement à l'année précédente, principalement attribuable à l'augmentation des demandes faites en vertu de la *Loi sur la protection des renseignements personnels*. Les demandes varient, de petites demandes de renseignements précis aux demandes plus générales nécessitant une consultation interministérielle. Quelle que soit la taille ou la complexité de la demande, la loi accorde aux ministères un délai de réponse de

30 jours. ACC ne respecte pas le délai de réponse de 30 jours dans environ 30 % des cas de demande officielle[1].

De nombreux risques et questions éventuels sont associés aux demandes relatives à l'AIPRP. Une récente demande présentée par un ancien combattant s'est traduite par une exposition médiatique accrue et un examen par la commissaire à la protection de la vie privée lorsqu'il a été jugé que certains employés avaient consulté de façon inappropriée un dossier. L'exposition médiatique défavorable s'est soldée par une augmentation notable des demandes relatives à l'AIPRP lorsque d'autres anciens combattants se sont inquiétés de l'accès à leur propre information. Il a été rapporté que l'augmentation de la charge de travail sans augmentation correspondante des ressources a eu des répercussions sur le bien-être des employés et a augmenté le risque d'erreur éventuelle créé en voulant respecter le délai de réponse de 30 jours prescrit par la loi.

Pour traiter adéquatement les demandes relatives à l'AIPRP, le Ministère dépend fortement de la capacité de tous les employés de classer l'information correctement. Cependant, nombre d'employés n'ont pas reçu une formation suffisante dans l'art de gérer l'information. Pour cette raison, il peut être compliqué de trouver l'information et par conséquent de répondre à la demande dans les délais prescrits, sans parler du risque accru d'information omise. De plus, le personnel chargé des demandes a de la difficulté à établir si l'information reçue concernant la demande est complète. Récemment, un cours intitulé « La gestion de l'information au travail – GI démystifiée » a été offert à certains employés pour les sensibiliser à leur rôle en gestion de l'information. On s'attend à ce que le cours continue à être offert à l'avenir.

D'ailleurs, pour améliorer la responsabilité liée à la collecte de l'information, le Ministère a mis en œuvre un nouveau processus entré en vigueur le 1er avril 2011. Le processus oblige les directeurs généraux des directions générales d'apposer leur signature pour confirmer que l'information assemblée est complète et pour déterminer l'information qui pourrait être délicate avant qu'elle soit acheminée à l'Unité de l'AIPRP. La politique et les procédures récentes d'ACC en matière de traitement des demandes d'accès aux documents et aux renseignements personnels en vertu de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels* aideront également à la prestation exacte et efficiente des services liés à l'AIPRP.

[1] Les détails du nombre de demandes et de leur délai d'exécution sont présentés dans les rapports annuels « Rapport sur la mise en application de la *Loi sur l'accès à l'information* » et « Rapport sur la mise en application de la *Loi sur la protection des renseignements personnels* ».

3.1.3 Évaluation des facteurs relatifs à la vie privée (72)

De nombreux risques et questions éventuels sont associés aux renseignements personnels qu'ACC gère. Afin de résoudre ces risques et questions éventuels, la Directive sur l'évaluation des facteurs relatifs à la vie privée (EFVP) du gouvernement fédéral exige que des EFVP soient menées pour les programmes nouveaux ou remaniés. L'EFVP est un processus systématique permettant de déterminer si les nouveaux systèmes d'information, programmes ou services administratifs, ou politiques et pratiques, ou ceux qui sont déjà en vigueur, se conforment aux exigences fondamentales en matière de protection de la vie privée. De plus, une EFVP aide à garantir le respect des lois relatives à la vie privée.

La Directive sur l'évaluation des facteurs relatifs à la vie privée exige qu'une EFVP soit exécutée avant que les institutions fédérales n'entreprennent tout nouveau projet qui pourrait avoir un effet négatif sur la vie privée des particuliers. L'élaboration d'une EFVP au cours des étapes de planification ou de développement initial d'un projet permet d'inclure la question de protection de la vie privée à la conception et à la mise en œuvre, de cerner les problèmes éventuels en matière de conformité et d'établir des stratégie pour la gestion du risque. Une fois achevée, l'EFVP peut également mener à un important remaniement des plans ministériels, en fonction des résultats de l'évaluation.

Étant donné l'accent mis par le Ministère sur son programme de transformation, le nombre d'EFVP requises augmentera au cours des prochaines années. Comme il faut des efforts conjugués pour l'élaboration des EFVP, les efforts du personnel demeureront substantiels. Une directive éventuelle pourrait mener au transfert de la responsabilité d'élaboration des EFVP aux unités opérationnelles tandis que la GI continuera d'offrir conseils et orientation sur ce processus complexe. Il faut souligner que la complexité liée à l'élaboration des EFVP est associée à une longue courbe d'apprentissage d'environ deux ans.

La récente plainte relative à la vie privée a sensibilisé ACC au besoin d'améliorer sa gestion de la protection des renseignements personnels de particuliers. Bien que la protection des renseignements personnels ne soit pas une science exacte, toute question concernant la vie privée est devenue délicate et comprend des répercussions plus importantes depuis la récente attention des médias envers les questions relatives à la vie privée. D'ailleurs, la tâche d'élaborer les EFVP est rendue plus difficile du fait que les Lignes directrices sur l'évaluation des facteurs relatifs à la vie privée du Conseil du Trésor sont énormément complexes et que la Politique d'évaluation des facteurs relatifs à la vie privée et les procédures connexes d'ACC sont très détaillées. S'y conformer, en plus de respecter la Directive sur l'évaluation des facteurs relatifs à la vie privée et les

Principes généralement reconnus en matière de protection des renseignements personnels n'est pas qu'une simple affaire.

3.1.4 Accès à l'information et protection des renseignements personnels (AIPRP) (69)

Les Canadiens ont besoin d'avoir accès à un vaste éventail de renseignements sur le gouvernement. Le public s'intéresse vivement à la transparence, voulant s'assurer que le gouvernement rend compte de ses objectifs et que les résultats peuvent être mesurés en fonction de ces objectifs. Du coup, cela rend le gouvernement plus responsable à l'égard des électeurs et facilite la participation informée du public à l'élaboration des politiques d'intérêt public.

Dans le cadre de ses activités quotidiennes, les ministères et les organismes du gouvernement fédéral recueillent des renseignements personnels de presque tous les Canadiens. La *Loi sur la protection des renseignements personnels* donne aux citoyens canadiens et aux personnes présentes au Canada le droit d'accès à leur information personnelle que le gouvernement fédéral a en sa possession. Elle protège également contre la divulgation non autorisée des renseignements personnels. De plus, elle précise strictement de quelle façon le gouvernement recueillera, utilisera, conservera, divulguera et supprimera tout renseignement personnel.

Le Bureau de l'AIPRP est consulté concernant les questions relatives à une variété de questions : sondages, questionnaires, problèmes de gestion de l'information, évaluations des facteurs relatifs à la vie privée, sécurité de l'information, mises en garde contre la divulgation de renseignements personnels, examen des ébauches de politiques, etc.

Le personnel doit posséder un savoir approfondi sur le traitement de l'information délicate et la détermination de l'information protégée ou classifiée. Le mauvais traitement de l'information peut entraîner la perte ou la diffusion de documents délicats. Le respect des règles prend du temps et retire à la prestation des services aux personnes et aux bénéficiaires l'attention qu'il faut lui apporter.

Depuis la récente plainte concernant la protection de la vie privée, la majorité des activités mettant en jeu la protection de la vie privée ont été évaluées comme étant des domaines à risque plus élevé. Pour atténuer ces risques, les contrôles sur l'accès aux systèmes d'information actuels ont été améliorés. De plus, les contrôles sur la saisie des données ont été modifiés en fonction du principe du « besoin de savoir ». Cela inclut de nouvelles politiques en matière de surveillance et de contrôle pour le RPSC. Des progrès notables ont été accomplis dans ce domaine depuis l'automne 2010.

La directive d'ACC sur la communication des renseignements personnels au ministre a été publiée en novembre 2010 à la suite de la plainte relative à la protection de la vie privée dans le but de prévenir les situations embarrassantes pour le ministre et le Ministère. Des séances de formation obligatoires sur le « besoin de savoir » ont été établies (environ 82 % des employés ont reçu la formation jusqu'à maintenant).

Une surveillance accrue de la part d'autres ministères gouvernementaux tel que le Commissariat à la protection de la vie privée s'est traduite par une vérification prochaine par la commissaire à la protection de la vie privée (automne 2011) et une évaluation externe annuelle (menée actuellement par Services de vérification Canada) sur le respect par ACC de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels* comme il est prévu dans le plan d'action en 10 points du ministre sur la protection de la vie privée. La surveillance a également mené à l'élaboration d'une nouvelle Infrastructure de protection des renseignements personnels qui a été créée en février 2011 dans le but de présenter le comité directeur de la protection des renseignements personnels, le chef de la protection des renseignements personnels et le coordonnateur de l'AIPRP.

3.2 Entités à risque moyen

3.2.1 Politiques relatives à la sécurité de la TI (60)

La politique sur la sécurité de la TI traite des contraintes exercées sur les fonctions, et les rapports entre elles, et également celles exercées sur l'accès par des systèmes externes et des particuliers. La sécurité de la TI fait partie intégrante d'une prestation continue des programmes et des services. Les ministères doivent considérer la sécurité de la TI comme une obligation opérationnelle puisque les intrusions peuvent entraîner une perte de service ou de confiance.

La Politique sur la sécurité du gouvernement précise les exigences relatives à la protection des biens du gouvernement, y compris l'information, et prescrit aux ministères et aux organismes fédéraux concernés d'avoir en place une politique sur la sécurité de la TI. La politique exigée peut être un document distinct ou des énoncés inclus à la politique ministérielle sur la sécurité. À tout le moins, une politique ministérielle sur la sécurité de la TI doit définir les rôles et les responsabilités du personnel de la TI. Elle doit également établir des liens avec d'autres politiques, normes et autres exigences réglementaires du Ministère qui ont rapport avec la sécurité de la TI.

La Politique sur la sécurité du gouvernement dérive de l'article 7 de la *Loi sur la gestion des finances publiques* qui accroît l'importance de la politique lorsqu'on considère la

nouvelle nature de la protection des renseignements personnels au sein du gouvernement. Les violations ou l'accès inapproprié aux systèmes informatiques d'ACC peuvent entraîner une interruption des activités ou même une panne complète de l'infrastructure de la TI. Certains employés peuvent également contourner les procédures de TI recommandées (et ne pas recevoir les mises à jour de sécurité essentielles) en n'éteignant pas leurs ordinateurs à la fin de la journée, ce qui est exigé par la Sécurité de la TI.

L'introduction de nouvelles technologies crée des risques éventuels consécutifs à la nécessité d'établir ou de mettre à jour les politiques relatives à la sécurité de la TI. Certaines politiques relatives à la TI d'ACC ne sont pas mises à jour de façon constante et les processus et procédures sont par conséquent incomplets. La Politique sur la sécurité du gouvernement (2009) remplace la Politique sur la sécurité (2002) et la Politique de gestion de l'infrastructure à clé publique du gouvernement du Canada (2004). Cependant, ACC œuvre à la mise à jour de ses politiques pour les harmoniser avec la Politique sur la sécurité du gouvernement. La rédaction et l'interprétation des politiques relatives à la sécurité de la TI requièrent un savoir exhaustif. Ce savoir est également important pour arriver à comprendre les dépendances ayant trait à l'intégration de systèmes et des logiciels appartenant aux entrepreneurs externes et aux autres ministères gouvernementaux.

3.2.2 Fonds de renseignements (46)

Le Fonds de renseignements est l'entité générale pour le service d'expert du Fonds de renseignements, le bureau des documents classés par sujets du Ministère, le service ministériel de dépôt des documents classés par sujets, les services régionaux de documents, le service Opérations - Documents des clients, la propriété de l'information, les périodes de rétention et les exigences liées aux documents.

Le Fonds de renseignements offre aux employés d'ACC des conseils et une orientation sur la façon d'organiser l'information (format papier ou électronique) et les obligations associées à la rétention et à la suppression de l'information.

Le projet pilote de numérisation de toute la correspondance d'arrivée d'ACC qui a lieu à Matane (Québec) occasionnera des changements importants aux procédures d'ACC concernant le Fonds de renseignements. Les documents d'arrivée d'ACC seront numérisés et entreposés à Matane par Travaux publics et Services gouvernementaux Canada (TPSGC) et les versions électroniques seront envoyées aux bureaux respectifs du Ministère. Cela entraîne des questions relatives à la communication de l'information à TPSGC, à l'entreposage et à la rétention de l'information dans les installations de

TPSGC à Matane. En outre, l'information pourrait être perdue ou égarée en cours de transport entre Matane et les bureaux d'ACC.

Anciens Combattants Canada a approuvé en principe un système de gestion des documents et de l'information électroniques (SGDIM), mais n'a pas les fonds voulus pour la mise en œuvre. Le Ministère dépend de plusieurs systèmes de gestion de l'information pour recueillir, protéger, analyser et gérer l'information. De nombreux employés ne sont pas sensibilisés à leurs responsabilités concernant les procédures de gestion de l'information. L'unité de la GI a récemment mis sur pied plusieurs projets de formation, y compris le cours « La gestion de l'information au travail – GI démystifiée » pour informer le personnel sur ses responsabilités.

3.2.3 Plan de continuité de la GI (46)

Le plan de continuité de la GI a pour objectif de définir les étapes à suivre dans l'éventualité où la version originale de documents est endommagée, détruite, perdue ou devient inaccessible. Le plan met l'accent sur le maintien des activités et la disponibilité de l'information à la suite d'une interruption et concerne l'opérations des dossiers des clients et les documents ministériels classés par sujet. Le plan de continuité de la GI est donc un volet important du plan de continuité des activités.

Le plan de continuité de la GI actuel d'ACC n'est pas suffisamment détaillé puisqu'il ne défini pas les obligations de rendre compte et les responsabilités des employés d'ACC. Des risques supplémentaires sont créés par l'insuffisance des pratiques exemplaires et de lignes directrices des organismes centraux et la charge accrue de travail pour le personnel de la GI et de la TI à la suite de la plainte relative à la protection des renseignements personnels.

Anciens Combattants Canada dépend fortement des systèmes informatiques pour recréer les documents sur support papier qui ont été perdus ou endommagés. De plus, la situation accroît l'importance d'un plan de continuité de la TI et d'un système de gestion des documents et de l'information électroniques.

D'ailleurs, le projet pilote de numérisation de toute la correspondance d'arrivée d'ACC qui prendra place à Matane (Québec) donnera lieu à l'apport de changements importants au plan de continuité de la GI d'ACC. Les documents d'arrivée d'ACC et de tous les autres ministères fédéraux seront numérisés et entreposés à Matane par TPSGC et les versions électroniques seront acheminées aux bureaux des ministères respectifs. En outre, l'information pourrait être perdue ou égarée en cours de transport entre les bureaux d'ACC et les installations de TPSGC.

3.2.4 Évaluations de la menace et des risques (38)

Comme il est précisé dans la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information en application de la Politique sur la sécurité du gouvernement, les évaluations de la menace et des risques (EMR) aident à définir les exigences en matière de sécurité que les ministères fédéraux doivent satisfaire pour garantir la sécurité de l'information et les biens de la TI dont ils ont la responsabilité.

Anciens Combattants Canada doit mener une EMR pour tous les programmes ou systèmes nouveaux ou modifiés. Les EMR peuvent être brèves et simples ou beaucoup plus détaillées et rigoureuses selon la vulnérabilité, l'importance ou la complexité du programme, du système ou du service évalué.

Les évaluations de la menace et des risques deviennent de plus en plus nécessaires à mesure de l'augmentation du nombre et de la gravité des menaces, des points délicats et des incidents. De plus, la TI ne cesse d'évoluer rapidement à l'appui d'une connectivité accrue et de la prestation améliorée des services. Tout le Ministère dépend d'un petit groupe de travail chargé des EMR au sein de l'unité de la Sécurité de la TI. Pour l'élaboration des EMR, les employés doivent connaître à fond la technologie et l'application connexe pour l'entité. Conformément à la transformation, l'unité de la Sécurité de la TI envisage d'accroître les ressources afin de composer avec la charge de travail additionnelle. Pour améliorer l'efficacité des EMR, le groupe de travail prévoit à l'avenir réaliser le suivi des recommandations des EMR.

3.3 Entités à risque faible

3.3.1 Gestion des formulaires (21)

L'Unité de la gestion des formulaires élabore les formulaires d'ACC, gère le processus d'approbation pour s'assurer que les formulaires respectent toutes les exigences du gouvernement du Canada et coordonne l'impression et le stockage des formulaires.

Le programme de transformation générera des modifications notables aux formulaires. De plus, le principe du « besoin de savoir » entraînera l'examen encore plus détaillé des formulaires et la détermination de l'exigence de certaines informations, créant ainsi une certaines inefficacités opérationnelles. En réponse, ACC a émis de nouvelles politiques et lignes directrices sur la gestion de l'information qui améliorent les processus relatifs à la gestion des formulaires.

3.3.2 Conseils et orientation (20)

Le personnel de la DSGI est prêt à fournir conseils et orientation sur toutes les questions relatives à la gestion de l'information, dont les suivantes : accès à l'information; protection des renseignements personnels (ceux des employés et des anciens combattants), exigences relatives aux documents, tenue des dossiers, gestion des formulaires, exigences relatives aux utilisateurs dont il faut tenir compte dans la conception des systèmes informatiques, propriété de l'information, conditions relatives à la GI dans les énoncés de travaux (EDT) et les contrats, délai de conservation et équipe de consultation sur les projets.

Dans le cadre du plan d'action en 10 points portant sur la protection des renseignements personnels et pour sensibiliser davantage les employés, la DSGI a mis sur pied plusieurs projets de formation sur la gestion de l'information comme la séance obligatoire sur le « besoin de savoir » (à laquelle 82 % du personnel a participé). De plus, le cours « La gestion de l'information au travail – GI démystifiée » a été offert aux employés de l'Administration centrale.

La pratique de la gestion de l'information doit être accompagnée d'une sensibilisation continue. Même si les employés d'ACC reçoivent actuellement de la formation, une formation additionnelle devra également être offerte de sorte que les pratiques exemplaires d'ACC en gestion de l'information sont appliquées. Bien que le service de conseils et d'orientation soit un service précieux pour tous les secteurs du Ministère et leurs employés, il pourrait être rétabli après une interruption dès la réinstallation.

3.3.3 Surveillance et prévention des pourriels (19)

Par définition, les pourriels sont des messages reçus ou envoyés qui n'avaient pas été sollicités. Les messages dont il est question n'ont aucun rapport avec le milieu de travail et visent souvent à vendre un produit ou un service. Pour prévenir efficacement les infiltrations par les pourriels et les virus éventuels, de nombreux logiciels ont été conçus de sorte à filtrer les pourriels. Le Ministère a été très proactif pour déterminer et prévenir les pourriels et autres messages nuisibles. De plus, le Ministère a établi un protocole pour éliminer tous les pourriels.

3.3.4 Conditions relatives à la GI dans les énoncés de travaux (EDT) et les contrats (16)

La DSGI s'assure que certaines exigences sont incluses dans les dispositions contractuelles à l'intention des entrepreneurs et autres personnes chargés de travaux au nom d'ACC. L'Unité de la GI s'assure également que les ententes voulues sont établies concernant l'information obtenue d'autres ministères et organismes fédéraux, de particuliers ou d'autres tiers qui ne font pas partie du gouvernement fédéral.

Les employés de la GI doivent connaître les lignes directrices et la législation connexe relatives aux contrats étant donné qu'ACC dépend énormément d'entrepreneurs externes et doivent s'assurer que les dispositions sont en place pour protéger l'information délicate. Comme la majorité de ces dispositions sont générales, l'entité est considérée comme étant à risque faible.

3.3.5 Révision et traduction (16)

Le bureau des réviseurs d'ACC offre des services de traduction à l'interne au Ministère à condition que le document ne dépasse pas 500 mots. Le document doit provenir d'un employé de l'Administration centrale et ne doit pas être communiqué à l'extérieur du portefeuille d'ACC. Son personnel révise également des documents dans les deux langues officielles et propose des améliorations aux documents. Le personnel compare les versions françaises et anglaises pour s'assurer que la traduction est correcte, que le style et la mise en page sont uniformes et que la grammaire, l'orthographe et la ponctuation sont corrects.

Le Bureau de la traduction de TPSGC offre aux ministères et organismes fédéraux des services de traduction de documents plus longs, des services d'interprétation et des services terminologiques dans les deux langues officielles. ACC a recours aux services de traduction de TPSGC dans le cas de documents très délicats, y compris les documents du Cabinet. Dans certains cas, en raison de contraintes temporelles, ACC ne transmet pas toujours les documents cotés par une méthode sécurisée. Jusqu'à maintenant, aucune intrusion n'a été détectée, mais en n'utilisant pas les méthodes sécurisées, le Ministère expose les documents délicats et classifiés au risque.

3.3.6 Bibliothèque (12)

La bibliothèque ministérielle d'ACC offre des services de bibliothèque complets au personnel de l'Administration centrale, des bureaux de district et des bureaux régionaux. De plus, les services de bibliothèque sont également offerts au Tribunal des anciens combattants (révision et appel) et sur place à Charlottetown au grand public. La collection de la bibliothèque porte principalement sur les sujets tels que l'histoire militaire, la santé et la gérontologie. Elle comprend également des publications ministérielles et autres documents gouvernementaux connexes et des textes de loi.

La perturbation des activités de cette entité aura des répercussions limitées sur les activités quotidiennes étant donné que la majorité des ressources sont disponibles sur Internet ou par le truchement d'autres organismes fédéraux ou de bibliothèques publiques. De plus, la non disponibilité de la bibliothèque aura peu de répercussions sur la prestation des services aux employés, aux anciens combattants ou à leur familles, et au public en général.

4.0 CONCLUSION

Depuis l'automne 2010, le Ministère a répondu avec énergie aux critiques du public ayant trait à la gestion de l'information. Des progrès notables ont donc été accomplis. Vu l'importance de la gestion de l'information et la sensibilité actuelle même après de tels progrès, la direction doit savoir que certaines activités continuent de représenter un risque élevé. En outre, l'équipe chargée de l'évaluation a cerné certains risques généraux au sujet desquels elle recommande à la direction de prendre des mesures correctives :

- L'absence d'un plan de continuité des activités de la TI éprouvé et entièrement fonctionnel expose le Ministère à un risque notable et pourrait mener à l'interruption de la prestation des services.

- L'absence d'un centre désigné des activités d'urgence expose le Ministère à risque dans l'éventualité d'un incident majeur.

- Le développement d'un système de gestion des documents et dossiers électroniques a été approuvé en principe, mais les fonds n'ont pas été obtenus. L'absence actuelle d'un tel système rend la saisie et la réception de l'information problématiques.

- Anciens Combattants Canada ne respecte pas le délai d'exécution de 30 jours pour les demandes d'accès à l'information et de protection des renseignements personnels (AIPRP), ce qui va à l'encontre de la *Loi sur l'accès à l'information.*

- Le plan actuel de continuité de la GI n'est pas suffisamment précis quand aux rôles, aux responsabilités et à l'obligation de rendre compte. Le processus d'envoi de l'information à Matane (Québec) et de retour de cette information accroît le risque de perte de l'information ou de son égarement, amplifiant l'importance d'un plan de continuité de la GI bien établi.

- La transformation a pour objectif la refonte de la prestation des services et la réduction de la complexité des programmes, d'où le besoin de mener des évaluations additionnelles des facteurs relatifs à la vie privée. Cela aura pour conséquence d'accroître la charge de travail et possiblement d'altérer les responsabilités.

Recommandation

Il est recommandé au sous-ministre adjoint, Services ministériels, de présenter les risques susmentionnés au Comité de la haute direction pour déterminer l'approche que le Ministère adoptera pour gérer ces risques.

Réponse de la direction

La direction accepte la recommandation. Des mesures seront prises pour inscrire l'évaluation des risques liés à la gestion de l'information à une réunion du Comité de la haute direction au cours des prochaines semaines. Une récente séance d'information sur la gestion de l'information offerte au CHD le 15 juin dernier a cependant mis en évidence de nombreuses préoccupations; les résultats de l'examen aideront à orienter les travaux qui doivent être accomplis au cours des prochains mois.

Plan d'action de la direction

Mesure corrective à prendre	Bureau de première responsabilité	Date cible
Première séance d'information sur la GI – Le point	GITI	Juin 2011
Séance d'information au CHD – Évaluation des risques liés à la GI	V et É, SMA des SM	Juillet 2011
Mise à jour de la stratégie en matière de GI et élaboration du plan de mise en œuvre	GITI	Septembre 2011
Mise en œuvre du plan en parallèle au programme de transformation	GITI	Mars 2014

5.0 DISTRIBUTION

Sous-ministre

Sous-ministre déléguée

Ombudsman des vétérans

Chef du cabinet du ministre

Membres du Comité ministériel de vérification

Sous-ministre adjoint, Services ministériels

Sous-ministre adjoint, Politiques, Communications et Commémoration

Sous-ministre adjoint, Prestation des services

Directeur général, Communications

Directeur général, Secrétariat du Ministère et Coordination des politiques

Directeur général, Ressources humaines

Directeur général, Gestion de l'information et Technologie de l'information

Avocat général, Services juridiques

Directeur exécutif et Chef avocat-conseil des pensions

Directrice exécutive de l’Hôpital Sainte-Anne

Directeur, Information, coordination et liaison

Directeur, Services de gestion de l’information

Directeur, Sécurité et services immobiliers

Conseillers exécutifs du sous-ministre

Bureau du contrôleur général (Registre de vérification interne)

Bureau du vérificateur général

APPENDICE 1 : ANALYSE DE L'EXPOSITION AU RISQUE – CLASSEMENT PONDÉRÉ

				Principaux facteurs de risque									
				Niveau et nouveauté du changement		Niveau de complexité		Exigence prévue par la loi ou autre exigence de conformité		Niveau de connaissances		Niveau de dépendance	
Rang	**Entité**	**Pondé-ration**	**Signifi-cation**	**P**	**I**	**P**	**I**	**P**	**I**	**P**	**I**	**P**	**I**
Entités à risque élevé													
1	Planification de la continuité des activités (incluant le plan de continuité des activités de la TI)	90	3	3	3	3	3	3	3	3	3	3	3
2	Demandes relatives à l'AIPRP	78	3	3	3	3	3	2	3	2	2	2	3
3	Évaluations des facteurs relatifs à la vie privée	72	3	2	3	2	3	1	3	2	3	2	3
4	Accès à l'info et protection des renseign. pers.	69	3	3	3	2	2	3	2	2	2	2	2
Entités à risque moyen													
5	Politiques sur la sécurité de la TI	60	3	2	2	2	1	2	2	2	2	2	3
6	Fonds de renseignements	46	2	3	2	2	2	1	3	2	3	2	3
7	Plan de continuité de la GI	46	2	3	3	3	3	2	2	1	2	2	2
8	Évaluations de la menace et des risques	38	2	2	2	2	2	1	3	2	2	1	2
Entités à risque faible													
9	Gestion des formulaires (DSGI)	21	1	2	3	1	3	1	3	2	2	2	2
10	Conseils et orientation (DSGI)	20	1	2	3	2	1	1	2	2	3	2	2
11	Surveillance et prévention des pourriels	19	1	3	2	2	2	1	1	2	2	2	2
12	Conditions relatives à la GI dans les EDT et les contrats	16	1	1	1	1	1	1	3	1	2	2	3
13	Révision et traduction	16	1	2	1	2	1	1	3	2	1	1	2
14	Bibliothèque	12	1	1	2	1	1	1	1	1	2	1	1

Légende : P = Probabilité; I = Incidence

3 = Élevée
2 = Moyenne
1 = Faible