Anciens Combattants Canada
Veterans Affairs Canada

Canada

Vérification du contrôle de l'accès aux systèmes

Direction générale de la vérification et de l'évaluation

Novembre 2024

ISBN 978-0-660-77360-5

Remerciements

L’équipe de vérification tient à remercier le personnel de la Direction générale de la technologie de l’information, de la gestion de l’information, de l’administration et de la protection des renseignements personnels d’Anciens Combattants Canada ainsi que le personnel de la Direction générale de la gestion des programmes et de la prestation des services. Leurs contributions ont été essentielles à la réussite de cette vérification.

Table des matières

Sommaire

Contexte

Anciens Combattants Canada (ACC) a la responsabilité de protéger les renseignements de nature délicate qu'il détient sur ses clients. La présente vérification visait à s'assurer que les systèmes et les contrôles sont conçus de manière à garantir que les personnes autorisées ont accès aux renseignements contenus dans certains systèmes (RPSC et GCcas-Pension à vie) de la manière appropriée. La période couverte s'étend du 1er janvier 2023 au 31 décembre 2023.

Principales constatations et conclusions

Nous avons constaté que des exigences et des procédures sont en place, mais qu'il existe une marge d'amélioration. Les privilèges d'accès sont définis à l'aide de matrices d'accès, qui établissent la relation entre les rôles et les autorisations ou niveaux d'accès qui leur sont accordés, mais les responsabilités relatives à ces matrices ne sont pas claires. Des changements sont nécessaires dans les contrôles internes des comptes d'administrateur du système dans le système Pension à vie.

Les utilisateurs reçoivent une formation et des rappels réguliers sur l'utilisation acceptable des systèmes, mais aucune communication à ce sujet n'est fournie au moment où l'accès leur est accordé. Il n'y a pas d'examen périodique des privilèges d'accès ni de surveillance régulière des activités des utilisateurs, bien que les systèmes enregistrent certaines activités des utilisateurs.

Dans l'ensemble, l'équipe de vérification a déterminé que ces contrôles internes doivent être améliorés. Nous n'avons trouvé aucune preuve de violation de la vie privée, car cela ne faisait pas partie des objectifs de la vérification. Toutefois, si les faiblesses relevées ne sont pas corrigées, les risques d'atteinte à la vie privée pourraient nuire à la réputation d'ACC. Les clients pourraient perdre confiance dans la capacité d'ACC à conserver et à gérer leurs renseignements personnels.

Recommandations

La vérification a donné lieu aux recommandations suivantes :

- Mettre à jour et approuver les procédures.
- Définir et communiquer les responsabilités relatives aux matrices d'accès.
- Améliorer les contrôles internes relatifs à l'accès des administrateurs du système dans le système Pension à vie.
- Informer les utilisateurs autorisés de l'utilisation acceptable au moment où l'accès leur est accordé.
- Effectuer un examen périodique des comptes utilisateurs et surveiller l'activité des utilisateurs.

Signature de la dirigeante principale de la vérification

Lindy McQuillan, CPA, CMA
Dirigeante principale de la vérification
Anciens Combattants Canada

1.0 Contexte

ACC dispose de plusieurs systèmes d'information qui contiennent des renseignements personnels et sensibles sur environ 180 000 clients. Le personnel, les entrepreneurs et les autres utilisateurs ont besoin d'accéder à ces renseignements pour fournir des services aux vétérans et à leur famille. Il incombe à ACC de protéger ces renseignements des accès non autorisés. Les systèmes et les contrôles doivent être conçus de manière à garantir que les personnes autorisées ont accès aux systèmes d'information de manière appropriée.

Deux des systèmes d'information les plus utilisés qui contiennent des renseignements sur les clients d'ACC sont le Réseau de prestation des services aux clients (RPSC) et GCcas-Pension à vie (Pension à vie)[1]. L'accès à ces systèmes est accordé par les agents de contrôle de l'accès (ACA) de la Direction des opérations de la TI. Pour obtenir l'accès, l'utilisateur soumet une demande (à l'aide du programme AssystNet) précisant le type d'accès requis (rôle/description de travail) et joignant la preuve de l'autorisation de son superviseur. Cette preuve prend généralement la forme d'un courriel, mais il existe d'autres méthodes, comme la soumission du registre AssystNet par le superviseur. L'ACA examine la demande, communique avec l'utilisateur si des renseignements sont manquants et vérifie les rôles/descriptions de travail dans la matrice appropriée. Une fois tous les renseignements requis fournis, l'ACA accorde l'accès aux systèmes et aux rôles/descriptions de travail demandés, à l'aide de l'Outil d'accès au système de l'utilisateur du RPSC (RPSC) ou de Dynamics 365 (Pension à vie).

Un courriel est envoyé à l'utilisateur pour confirmer que son accès a été accordé. Les utilisateurs peuvent alors uniquement voir et/ou modifier les renseignements contenus dans les rôles/descriptions de travail qui leur ont été attribués.

Il existe plusieurs façons de supprimer l'accès d'un utilisateur. Dans le RPSC, si la date de fin d'accès de l'utilisateur est connue, elle est saisie lors de la configuration de l'accès, et l'accès est automatiquement supprimé à la date de fin. Il n'existe aucune option similaire dans le système Pension à vie. Lorsque l'accès doit être modifié ou supprimé pour l'un ou l'autre système, une demande est soumise (par l'utilisateur ou son gestionnaire) détaillant les modifications à apporter. La demande est soumise à l'aide du programme AssystNet pour un utilisateur qui quitte le Ministère et demande la suppression de tous ses accès, et à l'aide d'un modèle de courriel pour un utilisateur qui change de service au sein du Ministère et demande une modification de ses accès. L'agent de contrôle de l'accès examine la demande et communique avec le demandeur si des renseignements manquent. Une fois tous les renseignements requis fournis, l'ACA modifie ou supprime l'accès à l'aide des mêmes programmes utilisés pour l'accorder.

[1] GCcas – Pension à vie était l'application utilisée au moment de la vérification. Après la période visée par la vérification, l'application Pension à vie a été transférée dans le nuage et est désormais désignée par le personnel des opérations de la TI sous le nom de « Pension à vie », qui sera utilisé tout au long du rapport de vérification. Bien que le processus pour les agents de contrôle de l'accès ait légèrement changé avec la migration, les conclusions du présent rapport demeurent toutes applicables.

2.0 Résultats de la vérification

En préambule aux résultats de la vérification, l'équipe de vérification tient à souligner que, bien que la vérification portait sur le RPSC et le système Pension à vie, des membres du personnel lui ont fait savoir que certaines des questions soulevées dans les sections suivantes ne concernent pas uniquement le RPSC et le système Pension à vie et que certaines d'entre elles seraient plus faciles à régler au stade de la conception du système. Nous encourageons donc la direction d'ACC à utiliser les constatations et les recommandations de la présente vérification pour aider à réduire les risques dans les autres systèmes d'information existants, ainsi que dans l'élaboration et l'amélioration des systèmes nouveaux et anciens (par exemple, dans le cadre du projet de modernisation de la TI en cours).

2.1 Exigences et procédures

Les exigences et les procédures sont en place, mais des lacunes ont été relevées et l'incohérence des documents utilisés pour approuver les demandes d'accès pose problème.

Pourquoi est-ce important?

Les exigences et les procédures constituent des contrôles internes importants, car elles établissent des règles claires sur la manière de préserver la sécurité et la confidentialité des renseignements critiques. Elles aident également les employés d'ACC à savoir ce qu'on attend d'eux, ce qui réduit les erreurs et la confusion. Dans l'ensemble, elles contribuent à créer un lieu de travail cohérent et efficace.

Ce que nous avons constaté

Les exigences en matière de contrôle de l'accès sont généralement établies dans les normes de sécurité pour le contrôle de l'accès d'ACC (ci-après appelées « les normes »). Cependant, les normes ont été élaborées en 2013 et contiennent certains renseignements désuets.

ACC a établi des procédures pour la création, la modification et la désactivation des comptes pour le RPSC et le système Pension à vie, mais certaines sont désuètes ou doivent être approuvées. Des lacunes ont été relevées dans les procédures fournies. En ce qui concerne la modification et la désactivation des comptes, des faiblesses ont été relevées dans la capacité à s'assurer que la Gestion de l'accès[2] est avisée lorsqu'un employé change de rôle ou quitte le Ministère.

[2] La Gestion de l'accès est l'équipe de la Direction générale de la technologie de l'information, de la gestion de l'information, de l'administration et de la protection des renseignements personnels qui assure l'accès, l'administration et le contrôle de la plupart des systèmes et des applications de technologie de l'information approuvés pour ACC.

Il n'existe pas de procédures pour l'examen périodique des comptes du RPSC et du système Pension à vie ni de processus documenté pour l'établissement de l'accès de l'administrateur du système[3] à l'environnement de production de la pension à vie.

Sur une note positive, la Gestion de l'accès a préparé un grand nombre de procédures. Bien que certaines soient désuètes et nécessitent une mise à jour, il existait de nombreux dossiers différents dans GCdocs qui semblaient bien organisés et contenaient toutes sortes de procédures pour différents scénarios.

Pour tester les contrôles internes existants, un échantillon de 172 nouveaux accès/demandes au RPSC et de 185 nouveaux accès/demandes au système Pension à vie a été testé. Nos tests de vérification visaient à déterminer si :

- les autorisations nécessaires avaient été obtenues pour accorder l'accès;
- l'accès a été accordé conformément à la demande.

Concernant le RPSC, nous avons constaté ce qui suit :

- 87 accès (50 %) étaient clairement accompagnés d'autorisations dans le registre (c'est-à-dire la demande). Parmi ceux qui n'avaient pas clairement obtenu d'autorisation, 37 accès (22 %) concernaient des employés d'un entrepreneur qui suit des procédures différentes ne permettant pas d'établir une piste de vérification claire de l'autorisation, 9 demandes d'accès (5 %) ont été annulées ultérieurement et 39 accès (23 %) semblaient avoir été autorisés, mais les preuves dans le dossier n'étaient pas claires (par exemple, la demande n'était pas suffisamment précise).

- 115 accès (67 %) avaient clairement des rôles appropriés attribués selon les registres. Parmi les éléments restants de l'échantillon, 14 (8 %) avaient des rôles attribués qui ne correspondaient pas aux registres, 9 (5 %) ont fait l'objet d'une annulation ultérieure de la demande et 34 (20 %) semblent avoir des rôles appropriés, mais les preuves n'étaient pas claires (par exemple, demande d'accès fondée sur la duplication d'un autre utilisateur).

Concernant le système Pension à vie, nous avons constaté ce qui suit :

- 90 accès (49 %) étaient clairement accompagnés d'autorisations dans le registre. Parmi ceux qui n'avaient pas clairement obtenu d'autorisation, 5 accès (3 %) n'avaient pas reçu l'autorisation appropriée, 77 accès (41 %) semblaient avoir été autorisés par un superviseur, mais les preuves n'étaient pas claires (par exemple, la demande n'était pas suffisamment précise) et, pour 13 éléments de l'échantillon (7 %), la vérification n'a pas permis de trouver de preuves permettant de tirer une conclusion, soit en raison de la manière dont l'accès avait été attribué, soit en raison de limitations des données (voir annexe A).

- 150 accès (81 %) avaient clairement des rôles appropriés attribués selon les registres. Parmi les éléments restants de l'échantillon, 14 (7 %) avaient des rôles attribués qui ne correspondaient pas aux registres, 3 (2 %) semblaient avoir des

[3] Les administrateurs du système ont généralement un accès beaucoup plus étendu aux systèmes que l'utilisateur moyen, car ils effectuent des tâches en arrière-plan telles que la programmation, l'attribution des droits d'accès, etc.

rôles appropriés, mais les preuves n'étaient pas claires (par exemple, les rôles demandés n'étaient pas suffisamment précis pour correspondre à la matrice) et pour 18 éléments (10 %), la vérification n'a pas permis de trouver de preuves permettant de tirer une conclusion, soit en raison de la manière dont l'accès avait été attribué, soit en raison de limitations des données (voir annexe A).

Plus généralement, nous avons constaté des incohérences dans la documentation obtenue pour l'approbation des demandes d'accès, ce qui rend difficile de conclure si les autorisations appropriées ont été accordées et si la Gestion de l'accès a accordé les accès appropriés.

Quelles sont les répercussions?

Il existe un risque que les décisions relatives à l'accès ne soient pas conformes aux attentes de la direction en raison de lacunes relevées dans les exigences et les procédures. De plus, ACC court un plus grand risque que des employés accèdent de façon inappropriée à des renseignements de nature délicate sur les vétérans en raison d'erreurs liées aux autorisations et à l'accès. ACC court également le risque que des employés d'un entrepreneur aient accès à des renseignements de nature délicate sur les vétérans en raison d'un faible processus d'approbation.

Recommandation 1

Le directeur général, Direction générale de la technologie de l'information, de la gestion de l'information, de l'administration et de la protection des renseignements personnels, devrait mettre à jour la documentation définissant les exigences en matière de contrôle de l'accès ainsi que les procédures relatives à la création, à la modification et à la désactivation de l'accès au RPSC et au système Pension à vie pour les utilisateurs internes et externes.

Réponse de la direction

La direction est d'accord avec cette recommandation. Nous réviserons et améliorerons notre documentation relative aux exigences et aux procédures afin d'y inclure des processus clairs pour la création, la modification et la désactivation de l'accès au RPSC et au système Pension à vie.

Cet effort nécessitera la collaboration de la TI et des intervenants en matière du RPSC et du système Pension à vie afin de s'assurer que la documentation est conforme aux procédures organisationnelles et aux processus d'approbation. Ces mesures combleront les lacunes actuelles des procédures et de la documentation et renforceront une approche cohérente et sécuritaire de la gestion du contrôle de l'accès au RPSC et au système Pension à vie.

Date d'achèvement visée : Décembre 2025

2.2 Définir les privilèges d'accès

Les privilèges d'accès sont définis à l'aide de matrice d'accès.

Les responsabilités visant à garantir que les matrices appliquent les principes du moindre privilège et de la répartition des tâches ne sont pas clairement définies.

Il existe une faiblesse dans les contrôles internes des comptes d'administrateur du système dans le système Pension à vie.

Pourquoi est-ce important?

Il est important de définir les exigences en matière d'accès en fonction des principes du moindre privilège et de la répartition des tâches afin de protéger les renseignements de nature délicate. Le principe du moindre privilège signifie que les individus ne doivent avoir accès qu'aux ressources dont ils ont besoin pour faire leur travail, ce qui réduit le risque de mauvaise utilisation accidentelle ou malveillante. La répartition des tâches garantit qu'aucune personne n'a le contrôle sur tous les aspects d'un processus critique, ce qui contribue à prévenir la fraude et les erreurs. Ensemble, ces principes créent un environnement plus sûr en minimisant les risques d'accès non autorisé et en favorisant la responsabilisation.

Nous nous attendions à ce qu'ACC ait établi des exigences pour la mise en œuvre de ces principes lors de la détermination des privilèges d'accès au RPSC et au système Pension à vie, et à ce que ces exigences aient été mises en œuvre.

Ce que nous avons constaté

Les normes de sécurité pour le contrôle de l'accès d'ACC indiquent que tous les systèmes doivent établir une répartition des responsabilités et séparer les tâches des personnes, au besoin, afin d'éliminer les conflits d'intérêts. Elles indiquent également que les systèmes et les applications doivent appliquer le principe du moindre privilège, en limitant l'accès autorisé des utilisateurs autant que nécessaire pour accomplir les tâches qui leur sont assignées. L'équipe de vérification a tenté de déterminer si ces exigences étaient respectées à l'aide des matrices propres à chaque système qui définissent les privilèges d'accès à attribuer aux utilisateurs.

Le RPSC et le système Pension à vie ont chacun une matrice conçue pour organiser et gérer les accès pouvant être attribués à chaque utilisateur dans chaque système. Les systèmes sont conçus pour appliquer les définitions d'accès dans les matrices, et la Gestion de l'accès utilise les matrices pour attribuer l'accès aux utilisateurs.

Les faits tirés de notre examen de chaque matrice sont présentés ci-dessous, suivis des conclusions générales, des répercussions et des recommandations.

RPSC

Matrice

La matrice du RPSC est un document complexe de plus de cinquante pages qui fournit des descriptions de travail et plusieurs niveaux d'accès pour chacune d'entre elles.

Il existe une liste connexe des autorités fonctionnelles, qui est un document identifiant les personnes à consulter en cas de modification de la matrice. La liste des autorités fonctionnelles est établie en fonction du nom et non du poste. Il est donc difficile de garantir que la liste soit mise à jour, car les personnes changent régulièrement de poste au sein de l'organisation. D'après les discussions avec certaines autorités fonctionnelles, celles-ci ne reçoivent aucune formation sur les responsabilités qui leur incombent en tant qu'autorités fonctionnelles et ne disposent que d'un minimum d'orientations. Ainsi, elles peuvent ne pas être conscientes de leur obligation de prendre en compte le principe du moindre privilège et la répartition des tâches lorsqu'elles approuvent des modifications apportées à la matrice.

La Gestion de l'accès déclare détenir la responsabilité administrative de la matrice, mais nous n'avons pas été en mesure de déterminer qui détient la responsabilité globale du contenu de la matrice. La liste des autorités fonctionnelles est un document de 19 pages contenant les noms des personnes responsables des différents niveaux d'accès, sans attribuer de responsabilité globale. Il est donc difficile pour ACC de s'assurer que la matrice traite avec précision les risques pour l'organisation en matière du moindre privilège, de la répartition des tâches et de l'accès inapproprié aux renseignements.

Sur une note positive, il existe des directives claires et précises sur la manière d'apporter des modifications à la matrice, qui comprend un processus d'approbation par les autorités fonctionnelles, avec une trace documentée des modifications demandées et des approbations. De plus, la matrice et la liste des autorités fonctionnelles sont disponibles dans les deux langues officielles et indiquent clairement qui est responsable des différents types d'accès au RPSC.

Moindre privilège

De nombreuses entrevues avec des employés ont révélé que l'on attribuait aux employés le moins d'accès possible pour faire leur travail, que le RPSC était très strictement contrôlé et que l'accès était accordé écran par écran. En témoigne la matrice elle-même, qui compte plus de 50 pages et fournit des descriptions de travail et plusieurs niveaux pour chacune d'entre elles. Lorsque l'accès est accordé, l'utilisateur a accès à tous les clients du système.

Pension à vie
Matrice La matrice bilingue Accès au système PFL est un document Excel d'environ deux pages relativement simple qui répertorie les groupes opérationnels et les rôles attribués à chacun d'entre eux. Toute modification est discutée avec le propriétaire du produit et d'autres personnes si nécessaire. Cependant, il n'y a pas de liste des personnes à consulter en cas de modifications ou pour obtenir des conseils sur les personnes à contacter. Il est donc difficile de savoir qui possède les connaissances et/ou l'autorité nécessaires pour apporter des changements. Il n'existe aucun processus documenté sur la manière d'apporter des modifications à la matrice, mais celles-ci sont consignées dans un registre avec une piste de vérification. La Gestion de l'accès déclare détenir la responsabilité administrative de la matrice, mais l'équipe de vérification n'a pas été en mesure de déterminer qui détient la responsabilité globale du contenu de la matrice. Il est donc difficile pour ACC de s'assurer que la matrice traite avec précision les risques pour l'organisation en matière du moindre privilège, de la répartition des tâches et de l'accès inapproprié aux renseignements. Sur une note positive, la matrice est disponible dans les deux langues officielles et documente clairement l'accès au système Pension à vie dont bénéficie chaque groupe opérationnel. L'équipe de vérification a relevé des exemples de modifications apportées à la matrice sans approbation officielle documentée, de modifications qui n'ont pas été reflétées en temps opportun et de sections de la matrice qui semblaient devoir être mises à jour. *Moindre privilège* De nombreuses personnes questionnées ont mentionné que l'accès au système Pension à vie était assez souple, le système reposant sur la conscience des employés quant aux renseignements auxquels ils peuvent avoir accès dans le cadre de leur travail. Cela dit, la matrice définit clairement les groupes opérationnels et leurs rôles d'accès. Nous avons été informés qu'une fois qu'un rôle est attribué, les utilisateurs ont accès à l'ensemble de l'application ou à plusieurs sections de l'application correspondant à ce rôle. Cependant, les utilisateurs doivent faire partie d'une équipe pour se voir attribuer du travail. Lorsque l'accès est accordé, l'utilisateur a accès à tous les clients du système. *Privilèges des administrateurs du système* Le rôle d'administrateur du système est introuvable dans la matrice et la Gestion de l'accès ne configure pas ces comptes dans le cadre de ses processus opérationnels normaux. Nous avons été informés que l'accès est accordé par le personnel informatique. Au 30 juin 2023, 63 noms d'utilisateur étaient enregistrés dans le système Pension à vie et associés à des rôles d'administrateur du système actifs. Les postes généralement associés aux noms des personnes associées à ces rôles étaient ceux du personnel travaillant dans le domaine des demandes des clients vétérans (c'est-à-dire, très probablement, des développeurs); le personnel travaillant dans la Gestion de l'accès (qui

Pension à vie
attribue l'accès aux autres utilisateurs); et les analystes des activités. Au moins 6 personnes disposaient de plusieurs noms d'utilisateur leur donnant accès en tant qu'administrateur du système. La plupart des noms d'utilisateur pour la Gestion de l'accès ont également le rôle d'administrateur des services de gestion de l'accès, mais le personnel de la Gestion des applications de TI nous a informés que ce rôle n'avait jamais été configuré pour accéder aux dossiers propres au système Pension à vie. L'équipe de vérification a été informée que les administrateurs du système ont plein accès aux données des clients et peuvent apporter des modifications au système dans l'environnement de production. L'équipe de vérification a été informée qu'à la suite de la vérification, l'accès des administrateurs du système avait été nettoyé. L'équipe a obtenu des données en date du 1er décembre 2024 et a relevé 28 noms d'utilisateur disposant d'un accès d'administrateur du système dans le système Pension à vie, ce qui semble plus raisonnable.

Dans le cas du RPSC et du système Pension à vie, nous avons trouvé des éléments indiquant que la répartition des tâches avait été prise en considération lors de l'élaboration des matrices (c'est-à-dire lors de la définition des privilèges d'accès). Il s'agissait notamment d'une liste de vérification du système Pension à vie et de quelques notes sur la matrice du système Pension à vie qui précisaient certains rôles à séparer. En ce qui concerne le RPSC, de nombreuses personnes interrogées ont confirmé que ce système était rigoureusement contrôlé, et nous avons obtenu certaines instructions destinées aux autorités fonctionnelles qui faisaient référence à la prise en compte de la répartition des tâches lors de l'approbation des modifications apportées à la matrice du RPSC. Cependant, nous n'avons pas trouvé de définition claire ni d'analyse de ce qu'ACC entendait par « fonctions qui devraient être séparées au sein de chaque système » afin de vérifier si elles étaient bien séparées. Par exemple, certains employés ont soulevé des préoccupations au sujet du personnel chargé des décisions relatives à l'indemnité supplémentaire pour douleur et souffrance (ISDS) en ce qui concerne le traitement des décisions et le paiement, mais il n'était pas clair si ACC avait entrepris une analyse pour déterminer s'il s'agissait vraiment d'un problème de répartition des tâches.

Comme indiqué ci-dessus, les deux matrices sont très différentes tant dans leur configuration que dans les processus de modification. Cela est tout à fait normal, car il s'agit de deux systèmes différents qui ont des rôles distincts et qui ont été mis en place à des moments différents. La vérification n'avait pas pour but d'évaluer si l'un ou l'autre des privilèges d'accès définis était meilleur que l'autre. Cependant, sans être en mesure de déterminer qui était responsable de chaque matrice, l'équipe de vérification n'a pas pu recueillir de renseignements sur la tolérance au risque d'ACC en ce qui concerne le rôle des matrices dans la protection de l'accès aux renseignements de nature délicate sur les clients. Il semblerait que la matrice du système Pension à vie accepte un niveau de risque plus élevé que la matrice du RPSC, et ACC devrait évaluer si cela correspond à son niveau de risque acceptable.

Quelles sont les répercussions?

Chaque système visé par la vérification contient des renseignements similaires et de nature délicate sur les clients. Cependant, les privilèges d'accès ont été définis de

manière très différente. Il existe un risque que l'un ou l'autre système ne respecte pas les seuils de tolérance au risque du Ministère. Étant donné qu'aucune responsabilité n'a été attribuée pour les matrices, il existe un risque accru que des modifications inappropriées ou non autorisées soient apportées aux matrices sans tenir compte des concepts requis du moindre privilège ou de la répartition des tâches.

Le manque de contrôle de l'accès des administrateurs du système Pension à vie pose un risque tant pour la cybersécurité que pour la sécurité interne. Les cybercriminels savent que les administrateurs du système ont un accès encore plus étendu que les utilisateurs ordinaires, ce qui en fait une cible de choix. Au sein de l'organisation, il existe un risque que les administrateurs du système abusent de leurs pouvoirs.

Recommandation 2

Le directeur général de la Gestion des programmes et de la prestation des services, en collaboration avec le directeur général de la Technologie de l'information, de la Gestion de l'information, de l'Administration et de la Protection des renseignements personnels, devrait définir et communiquer qui est responsable des matrices de contrôle d'accès pour le RPSC et le système Pension à vie et ce que ces responsabilités impliquent.

Réponse de la direction

La direction est d'accord avec cette recommandation. ACC a établi les rôles et les responsabilités liés aux systèmes destinés aux clients, tels que le RPSC et GCcas (Pension à vie). Nous tirerons parti de ces responsabilités existantes pour garantir l'attribution des responsabilités pour les matrices. ACC veillera à ce que la clarification et la communication des tâches précises soient assurées auprès de tous les intervenants et partenaires.

Date d'achèvement visée : Mars 2026

Recommandation 3

Le directeur général, Technologie de l'information, Gestion de l'information, Administration et Protection des renseignements personnels, devrait élaborer et mettre en œuvre un processus d'attribution des droits d'accès d'administrateur du système dans le système Pension à vie, examiner la liste des utilisateurs actuels qui ont des droits d'accès d'administrateur du système, supprimer les utilisateurs inutiles de ce rôle et ajouter le rôle à la matrice.

Réponse de la direction

La direction est d'accord avec cette recommandation. Nous mettrons en place un processus pour demander, approuver et attribuer des privilèges élevés dans le système Pension à vie et veillerons à ce que toutes les parties concernées en soient informées. Nous procéderons à un examen des utilisateurs actuels disposant d'un accès d'administrateur du système et supprimerons les utilisateurs qui n'ont plus

besoin de ce rôle, le cas échéant. Nous ajouterons le rôle d'administrateur du système à la matrice de contrôle d'accès.

Date d'achèvement visée : Juin 2025

2.3 Utilisation acceptable

Les utilisateurs reçoivent une formation et des rappels réguliers sur les règles d'utilisation acceptable. Cependant, au moment où ils deviennent utilisateurs autorisés de ces deux systèmes, aucune communication ne leur est transmise concernant l'utilisation acceptable propre à l'accès qu'ils viennent d'obtenir.

Pourquoi est-ce important?

Il est important d'informer les utilisateurs autorisés de l'utilisation acceptable des systèmes d'information du gouvernement afin de garantir la protection et l'utilisation responsable des données électroniques des clients. En définissant clairement ce qui est autorisé et ce qui ne l'est pas, nous contribuons à prévenir toute utilisation abusive, accidentelle ou intentionnelle des renseignements de nature délicate. Il s'agit notamment de protéger les renseignements personnels des clients, d'assurer la sécurité et de respecter les lignes directrices juridiques et éthiques. Lorsque les utilisateurs comprennent ces règles, cela réduit le risque de fuites de données, d'accès non autorisés ou d'autres erreurs susceptibles de nuire aux clients ou au gouvernement. Une formation adéquate et une bonne communication permettent à chacun de connaître son rôle dans la protection des renseignements auxquels il a accès dans le cadre de son travail.

Ce que nous avons constaté

Les nouveaux employés reçoivent des renseignements et une formation lorsqu'ils se joignent au Ministère. Par la suite, peu de formation de suivi ou de recyclage est offerte, sauf si un employé doit suivre la formation initiale en matière de sécurité une deuxième fois (par exemple, si sa carte de sécurité expire). Une formation supplémentaire en matière de sécurité et de sensibilisation fait l'objet d'un suivi et de rapports dans le cadre de la mise en œuvre du plan de sécurité ministériel (principalement pour les personnes qui obtiennent une nouvelle carte d'identité ou une carte mise à jour).

L'examen des contrats a été jugé hors de la portée de la vérification, mais nous avons demandé si les utilisateurs externes non gouvernementaux les plus importants[4] du RPSC recevaient des renseignements sur l'utilisation acceptable des systèmes d'information du gouvernement pour accéder aux données électroniques des clients.

[4] Les utilisateurs externes comprennent les entrepreneurs et autres intervenants extérieurs à ACC qui ont besoin d'accéder aux systèmes d'information pour remplir les exigences de leur contrat ou de leur entente.

Nous avons été informés que l'entreprise externe dispose d'un programme de formation obligatoire sur la sensibilisation à la sécurité et à la confidentialité, qu'elle opère dans le cadre d'une politique de sécurité d'entreprise et que ses procédures opérationnelles normalisées répondent aux exigences du contrat en matière de sécurité.

À ACC, tous les 120 jours, les utilisateurs doivent accepter un message contextuel sur l'utilisation acceptable, qui comprend un rappel que les employés ne doivent accéder aux renseignements confidentiels ou personnels que s'ils en ont véritablement besoin pour s'acquitter de leurs fonctions, et cette acceptation est consignée dans un registre. ACC organise chaque année une semaine de sensibilisation à la sécurité et au droit de savoir afin de rappeler au personnel qu'il ne doit pas accéder aux systèmes contenant des renseignements personnels sans besoin de savoir, et a envoyé des rappels dans les faits saillants du vendredi et dans d'autres courriels destinés au personnel.

Toutefois, au moment d'accorder l'accès au système, la Gestion de l'accès ne communique pas avec l'utilisateur pour s'assurer qu'il comprend ses responsabilités en matière d'accès aux renseignements sur les clients.

Quelles sont les répercussions?

Le fait de se fier à la formation initiale et aux rappels généraux ultérieurs comporte le risque que les utilisateurs qui accèdent à des données de nature délicate sur les clients n'accordent pas à ces renseignements toute l'importance qu'ils méritent. Il existe un risque que, lors de l'intégration des employés, le personnel soit « surchargé d'informations » et ne puisse pas établir de lien direct entre l'importance des données de nature délicate des clients et son travail. Si le courriel qu'ils reçoivent lorsqu'ils obtiennent l'accès souligne l'importance de cette mesure, ils seront peut-être mieux à même de comprendre et donc de se rappeler de n'accéder aux données de nature délicate sur les clients qu'en cas de nécessité.

Recommandation 4

Le directeur général, Technologie de l'information, Gestion de l'information, Administration et Protection des renseignements personnels, devrait mettre en œuvre un processus visant à informer les utilisateurs autorisés de l'utilisation acceptable du RPSC et du système Pension à vie au moment où l'accès à ces systèmes leur est accordé ou modifié.

Réponse de la direction

La direction est d'accord avec cette recommandation. Pour remédier à cela, nous inclurons une communication appropriée sur l'utilisation acceptable lorsque l'accès est accordé ou modifié. Ces efforts permettront de sensibiliser davantage les utilisateurs, de promouvoir la responsabilisation et d'atténuer les risques liés à une utilisation inacceptable.

Date d'achèvement visée : Juin 2025

2.4 Examen des accès

ACC n’effectue pas d’examen périodique des privilèges d’accès.

Pourquoi est-ce important?

Il est important de revoir régulièrement l’accès aux systèmes informatiques afin de s’assurer que seules les personnes autorisées ont accès aux renseignements de nature délicate. Au fil du temps, les employés peuvent changer de poste, quitter le Ministère ou ne plus avoir besoin de certaines autorisations. Si l’accès n’est pas mis à jour ou supprimé lorsqu’il n’est plus nécessaire, cela peut créer des risques pour la sécurité. En examinant et en ajustant périodiquement les droits d’accès, ACC peut réduire le risque d’accès non autorisé et s’assurer que les renseignements de nature délicate ne sont accessibles qu’aux personnes qui en ont besoin pour faire leur travail.

Ce que nous avons constaté

Il n’existe aucune procédure permettant à la Gestion de l’accès d’examiner régulièrement les accès afin de déterminer s’ils doivent être supprimés. Lorsque la Gestion de l’accès accorde l’accès au RPSC, des processus sont en place pour mettre fin automatiquement à l’accès à une date précise, mais cette fonctionnalité n’existe pas dans le système Pension à vie.

ACC n’examine pas périodiquement les privilèges d’accès. Ceux-ci sont plutôt révisés au besoin, lorsque des problèmes surviennent. Dans ce cas, on examine s’il s’agit d’un problème systémique lié au poste et on prend les mesures nécessaires.

L’équipe de vérification a procédé à une analyse des données et à un échantillonnage discrétionnaire afin de déterminer s’il y avait des utilisateurs dont l’accès devait être supprimé. Les constatations sont présentées ci-dessous. Il convient de noter qu’il ne s’agissait pas d’un examen complet de tous les accès des utilisateurs ni d’un échantillon statistique.

RPSC *Externe* Nous n’avons pas été en mesure de vérifier si l’accès des utilisateurs externes au RPSC aurait dû être supprimé en raison de l’absence de contrôles. Le personnel a suggéré de communiquer avec les utilisateurs externes pour confirmer qu’ils sont toujours employés. Toutefois, afin de réduire le risque d’accès non autorisé au RPSC, ACC devrait avoir cette information à l’interne plutôt que de compter sur les intervenants externes pour l’aviser du moment où l’accès doit être retiré. *Interne* Pour les autres utilisateurs internes du RPSC, la plupart des quarante-cinq éléments échantillonnés semblaient avoir un accès conforme à leur poste. Nous avons trouvé des preuves dans trois éléments de l’échantillon indiquant que certains accès auraient dû être supprimés. Au cours de la phase de planification de la vérification, nous avons également identifié deux membres de l’équipe de vérification qui disposaient d’un accès supplémentaire provenant de responsabilités antérieures et qui n’avait pas été supprimé. Nous avons également identifié une personne interrogée dans le cadre de la vérification qui avait un accès qui aurait dû lui être retiré.	**Pension à vie** *Externe* Nous n’avons pas été en mesure de vérifier si l’accès des utilisateurs externes au système Pension à vie aurait dû être supprimé en raison de l’absence de contrôles. Le personnel a suggéré de communiquer avec les utilisateurs externes pour confirmer qu’ils sont toujours employés. Toutefois, afin de réduire le risque d’accès non autorisé au système Pension à vie, ACC devrait avoir cette information à l’interne plutôt que de compter sur les intervenants externes pour l’aviser du moment où l’accès doit être retiré. *Interne* Pour les autres utilisateurs internes du système Pension à vie, nous avons trouvé des preuves dans deux des trente éléments échantillonnés que certains accès auraient dû être supprimés. Au cours de la phase de planification de la vérification, nous avons également identifié trois membres de l’équipe de vérification qui disposaient d’un accès supplémentaire provenant de responsabilités antérieures et qui n’avait pas été supprimé. Nous avons également identifié une personne interrogée dans le cadre de la vérification qui avait un accès qui aurait dû lui être retiré. Nous avons relevé 78 rôles d’accès (52 personnes) qui avaient une adresse courriel se terminant par @canada.ca plutôt que par @veterans.gc.ca. Nous en avons examiné huit, et il semblerait que tous soient des comptes auxquels l’accès aurait dû être retiré lorsque l’employé a quitté ACC. Il convient de noter que dans la plupart des cas, les comptes utilisateurs ont été supprimés, ce qui réduit le risque d’accès non autorisé. Après la période visée par la vérification, l’accès a été retiré aux 78 noms d’utilisateur qui avaient été relevés.

Quelles sont les répercussions?

Étant donné que les normes de sécurité pour le contrôle de l'accès (les normes) sont désuètes et qu'il n'existe aucun processus opérationnel pour l'examen des comptes, comme l'exigent les normes, le personnel est moins susceptible d'accorder la priorité à ces examens et peut les considérer comme moins importants. Le personnel responsable devrait non seulement procéder à l'examen des comptes, mais aussi créer le cadre nécessaire à cet examen, ce qui entraînerait une charge de travail supplémentaire.

Il existe un risque que l'accès des utilisateurs soit maintenu alors qu'il n'est plus nécessaire, ce qui leur permettrait d'accéder à des renseignements dont ils n'ont pas besoin pour s'acquitter de leurs fonctions actuelles. Il existe un risque accru d'accès inapproprié à des renseignements de nature délicate concernant les clients.

Recommandation 5

Le directeur général, Technologie de l'information, Gestion de l'information, Administration et Protection des renseignements personnels, devrait définir, documenter et mettre en œuvre un processus opérationnel pour l'examen périodique des comptes d'utilisateurs dans le RPSC et le système Pension à vie.

Réponse de la direction

La direction est d'accord avec cette recommandation. Pour remédier à cette situation, nous mettrons en place un processus d'examen cyclique dans le cadre duquel les autorités responsables de l'accès aux comptes du RPSC et du système Pension à vie examineront et confirmeront périodiquement que les niveaux d'accès attribués restent appropriés.

Date d'achèvement visée : Juin 2026

2.5 Surveillance

ACC n'a pas élaboré ni mis en œuvre de lignes directrices à l'intention du personnel pour surveiller les activités des utilisateurs dans le RPSC et le système Pension à vie, et aucun rapport automatique n'est généré. La surveillance est effectuée de façon ponctuelle, au besoin.

Pourquoi est-ce important?

Les procédures obligatoires du gouvernement du Canada en matière de contrôle de la sécurité de la TI stipulent que les ministères doivent créer, protéger et conserver les registres et les dossiers de vérification des systèmes d'information afin de permettre, entre autres, la surveillance de chaque système. Une surveillance active peut permettre de détecter les menaces et les incidents, réduisant ainsi le risque d'accès non autorisé aux renseignements de nature délicate des clients. Nous nous attendions à ce qui suit :

- Le RPSC et le système Pension à vie ont été programmés pour surveiller l'accès et l'activité des utilisateurs et produire des rapports réguliers.

- Des politiques ou des processus opérationnels étaient en place pour la surveillance des registres de vérification.
- Le personnel surveillait régulièrement l'accès conformément aux exigences prédéfinies.

Ce que nous avons constaté

D'après nos entrevues, ACC n'a pas établi de politique ni de processus opérationnel en matière de registre de vérification qui guiderait la surveillance des activités des utilisateurs dans le contexte des risques et des systèmes d'ACC (le RPSC et le système Pension à vie aux fins du présent rapport). Les développeurs de systèmes d'ACC ont configuré le RPSC et le système Pension à vie afin de déterminer quels champs sont consultés par quels utilisateurs, ce qui permet de surveiller les activités des utilisateurs. Cependant, les systèmes ne sont pas configurés pour générer automatiquement des rapports pouvant être utilisés à des fins de surveillance. Les rapports doivent être demandés au cas par cas.

Après avoir mené de nombreuses entrevues, nous n'avons trouvé aucune preuve d'une surveillance active des activités des utilisateurs du RPSC et du système Pension à vie. Des rapports ponctuels sont rédigés ou exécutés selon les besoins (par exemple, lorsqu'un incident de sécurité doit faire l'objet d'une enquête).

Quelles sont les répercussions?

En l'absence de politique ou de processus opérationnels exigeant une surveillance, le personnel est moins susceptible d'accorder la priorité à la surveillance et peut la percevoir comme moins importante que d'autres responsabilités. Il est difficile pour le personnel de surveiller l'accès des utilisateurs sans rapports générés automatiquement. Le personnel responsable devrait non seulement procéder à la surveillance, mais aussi créer le cadre nécessaire à cette surveillance, ce qui entraînerait une charge de travail supplémentaire.

En ne surveillant pas activement les activités des utilisateurs dans le RPSC et le système Pension à vie, il existe un risque que des accès inappropriés à des renseignements de nature délicate sur les clients passent inaperçus, ce qui pourrait entraîner des atteintes à la vie privée.

Recommandation 6

Le directeur général, Technologie de l'information, Gestion de l'information, Administration et Protection des renseignements personnels, devrait définir, documenter et mettre en œuvre un processus opérationnel pour permettre de surveiller et d'analyser les activités des utilisateurs dans le RPSC et le système Pension à vie et de créer des rapports à cet égard.

Réponse de la direction

La direction est d'accord avec cette recommandation. Un processus opérationnel sera élaboré pour surveiller régulièrement l'accès aux renseignements de nature délicate contenus dans le RPSC et le système Pension à vie. Le processus comprendra une enquête administrative appropriée et un suivi lorsque cela sera justifié. La formation et la sensibilisation feront également partie de la solution afin de

renforcer l'importance du besoin de savoir tout en permettant aux utilisateurs d'exercer efficacement leurs fonctions.

Date d'achèvement visée : Décembre 2025

2.6 Opinion de l'équipe de vérification

L'opinion de l'équipe de vérification est fournie en fonction de la portée de la vérification afin d'assurer la conformité aux éléments de la Directive sur la gestion de la sécurité du gouvernement du Canada. Les objectifs de la vérification portent sur la limitation de l'accès des utilisateurs aux données électroniques des clients et la surveillance de cet accès. Deux des principaux systèmes d'information d'ACC, Pension à vie et RPSC, ont été inclus dans la vérification.

ACC dispose de certains contrôles internes visant à limiter l'accès des utilisateurs aux données électroniques des clients, mais ces contrôles présentent des lacunes. Les exigences et les procédures relatives à l'octroi, à la modification et à la suppression de l'accès au RPSC et au système Pension à vie doivent être améliorées. Il est nécessaire de clarifier les responsabilités et d'améliorer les processus afin de définir les rôles en matière d'accès, y compris ceux des administrateurs du système. De plus, ACC n'effectue pas d'examens périodiques de l'accès des utilisateurs, comme il est requis. En ce qui concerne la surveillance de l'accès des utilisateurs, ACC a mis en œuvre certaines mesures pour permettre la surveillance des activités des utilisateurs, mais ces mesures présentent des lacunes et aucune surveillance n'est actuellement effectuée. Dans l'ensemble, l'équipe de vérification a déterminé que ces contrôles internes clés doivent être améliorés.

Dans chaque section susmentionnée, les répercussions des faiblesses du contrôle interne ont été cernées. Nous n'avons trouvé aucune preuve de violation de la vie privée, car cela ne faisait pas partie des objectifs de la vérification. Toutefois, si les faiblesses relevées ne sont pas corrigées, les risques d'atteinte à la vie privée pourraient nuire à la réputation d'ACC. Les clients pourraient perdre confiance dans la capacité d'ACC à conserver et à gérer leurs renseignements personnels.

La vérification est conforme aux Normes internationales pour la pratique professionnelle de l'audit interne de l'Institut des auditeurs internes, comme en témoignent les résultats du programme d'assurance et d'amélioration de la qualité. Les constatations et conclusions de la vérification contenues dans le présent rapport sont fondées sur des éléments probants suffisants et appropriés recueillis conformément aux normes applicables. Les opinions exprimées dans le présent rapport sont fondées sur les conditions qui existaient au moment de la vérification et ne s'appliquent qu'à l'entité examinée.

Annexe A – Au sujet de la vérification

Portée et objectifs

La vérification portait sur les contrôles internes en place entre le 1er janvier 2023 et le 31 décembre 2023 afin de s'assurer de leur conformité avec les éléments de la Directive sur la gestion de la sécurité du gouvernement du Canada pertinents aux objectifs énoncés. L'équipe de vérification a déterminé les systèmes d'information qui contiennent des renseignements sur les clients et qui présentent des risques liés au contrôle d'accès à inclure dans la vérification. La vérification portait sur deux des principaux systèmes d'information d'ACC, soit le système Pension à vie et le RPSC. Bien qu'un projet de modernisation de la TI soit en cours, il s'agit d'un projet à long terme dans le cadre duquel il pourrait être nécessaire d'envisager des contrôles d'accès au système. Par conséquent, les recommandations issues de cette vérification devraient encore pouvoir apporter une valeur ajoutée au Ministère à l'avenir.

Tous les autres systèmes d'information étaient exclus de la vérification. La vérification ne portait pas sur les contrôles de sécurité, la classification et le marquage liés à la sécurité, la sécurité physique, la cybersécurité, l'évaluation et l'autorisation en matière de sécurité, les contrôles des mots de passe ni les contrôles propres à l'accès de la Légion royale canadienne.

La vérification a pour objectif d'évaluer les mesures prises par ACC pour protéger les renseignements électroniques sur les clients contre l'accès non autorisé par le personnel et les autres utilisateurs du système. La vérification visait à répondre aux questions suivantes :

ACC a-t-il mis en place des contrôles internes pour s'assurer que l'accès aux données électroniques des clients est limité aux utilisateurs autorisés qui ont besoin d'y avoir accès?

ACC a-t-il mis en œuvre des contrôles internes pour créer des registres et des dossiers de vérification des systèmes d'information afin de permettre la surveillance et la production de rapports pour chaque système?

Critères de la vérification

Objectif 1

ACC a-t-il mis en place des contrôles internes pour s'assurer que l'accès aux données électroniques des clients est limité aux utilisateurs autorisés qui ont besoin d'y avoir accès?

Critères

a) ACC a établi des exigences et des procédures pour la création, la modification, l'examen périodique et la désactivation des comptes donnant accès à des données électroniques.

b) ACC définit les privilèges d'accès en fonction des exigences ministérielles en matière de sécurité et des principes du moindre privilège[5] et de la répartition des tâches.
c) ACC informe les utilisateurs autorisés de l'utilisation acceptable des systèmes d'information du gouvernement pour accéder aux données électroniques des clients.
d) ACC examine périodiquement les privilèges d'accès et supprime l'accès lorsqu'il n'est plus nécessaire.

Objectif 2

ACC a-t-il mis en œuvre des contrôles internes pour créer des registres et des dossiers de vérification des systèmes d'information afin de permettre la surveillance et la production de rapports pour chaque système?

Critères

a) ACC a mis en œuvre des mesures permettant de surveiller les activités des utilisateurs afin de s'assurer que ceux-ci sont responsables de leur accès aux données électroniques des clients.
b) ACC surveille l'utilisation acceptable de l'accès aux données électroniques.

Limites

La vérification a été limitée parce que nous n'avons pas pu accéder à Dynamics 365, accès qui était nécessaire pour effectuer un examen complet. Les rôles d'utilisateur que la Gestion de l'accès a pu fournir à l'équipe de vérification auraient donné aux vérificateurs un accès en écriture, ce qui aurait posé un risque inutile que l'équipe apporte des modifications accidentelles au système. Sans accès à ce système, l'équipe devait s'appuyer sur des rapports de données pour évaluer certains domaines. Par conséquent, les éléments probants issus de la vérification sont moins fiables pour les conclusions relatives au test de nouvel accès au système Pension à vie (section 2.1) et au test de retrait de l'accès au système Pension à vie (section 2.4).

Les données utilisées pour extraire des échantillons de nouveaux utilisateurs dans le cadre de la période couverte par les deux systèmes étaient limitées. Deux ensembles de données étaient disponibles, mais aucun ne couvrait tous les risques relevés par l'équipe de vérification. Ainsi, deux ensembles de données ont été combinés, les doublons ont été supprimés et un échantillon a été sélectionné à partir du rapport combiné. Nous n'avons pas été en mesure de vérifier l'exhaustivité ni l'exactitude du rapport combiné.

Pour un ensemble de données du RPSC, nous avons reçu cinq versions différentes au cours de notre vérification. Bien que les données finales semblaient exactes et pouvaient être utilisées dans le cadre des tests, nous n'avons pas été en mesure d'obtenir une assurance absolue quant à leur exactitude.

[5] Le principe du moindre privilège consiste à n'autoriser que les accès nécessaires aux utilisateurs pour accomplir les tâches qui leur sont assignées.

La vérification a été soumise à certaines restrictions en raison de l'ampleur et de la nature technique des questions examinées. Malgré tous nos efforts, certains aspects de la vérification n'ont pu être entièrement vérifiés et nous nous sommes fiés aux opinions de plusieurs personnes interrogées pour confirmer que certaines choses se produisaient dans les systèmes d'information. Dans un autre cas, nous avons vérifié l'existence de rapports à l'aide de données, mais nous n'avons pas testé leur adéquation.

Il est important de noter que les limites susmentionnées peuvent avoir eu une incidence sur certaines des conclusions de la vérification, mais nous n'avons relevé aucune limite susceptible d'avoir une incidence sur l'opinion ou les recommandations issues de la vérification.

Méthodologie

Méthode	Objectif
Entrevues	Poser des questions sur les processus en place pour définir et mettre en œuvre les exigences en matière d'accès, communiquer aux utilisateurs l'utilisation acceptable des systèmes d'information, les processus et la fréquence de révision des privilèges d'accès, les processus de détermination et de mise en œuvre des changements dans les privilèges d'accès en raison d'un transfert ou d'un départ. Poser des questions sur les processus décisionnels et les responsabilités en matière de matrices de contrôle d'accès. Poser des questions sur les processus en place pour accorder l'accès aux rôles d'administrateur du système. Poser des questions sur l'élaboration de systèmes permettant de surveiller l'accès, les processus et la fréquence de la surveillance des registres de vérification.
Observation directe	Observer les procédures de la Gestion de l'accès pour accorder l'accès à chaque système. Observer la connexion des utilisateurs à chaque système.
Examen de la documentation	Examiner la documentation relative aux processus afin d'étayer les réponses aux entrevues. Examiner les matrices d'accès des utilisateurs en place afin de garantir le respect du principe du moindre privilège et la répartition des tâches.

Méthode	Objectif
	Examiner les documents qu'ACC utilise pour informer les utilisateurs autorisés de l'utilisation acceptable des systèmes d'information du gouvernement pour accéder aux données électroniques des clients.
Examen des dossiers	Utiliser un échantillon de nouveaux accès accordés pour vérifier si les procédures ont été respectées et si l'accès a été accordé conformément à la demande d'accès approuvée. Utiliser un échantillon d'accès en place à un moment donné pour déterminer si l'accès aurait dû être supprimé.
Analyse des données	À l'aide de la liste des utilisateurs actuels pour chaque système, analyser les données sur les utilisateurs externes (extérieurs à ACC) et les administrateurs du système.

Annexe B – Classement des risques liés à l’opinion de vérification

Les définitions suivantes sont utilisées pour classer l’opinion de vérification présentée dans ce rapport.

Bien contrôlé	Seules certaines faiblesses insignifiantes relatives aux objectifs de contrôle ou à la bonne gestion de l’activité vérifiée sont relevées.
Généralement acceptable	Les faiblesses relevées, prises individuellement ou collectivement, ne sont pas importantes ou des mécanismes compensatoires sont en place. Les objectifs de contrôle ou la bonne gestion de l’activité vérifiée ne sont pas compromis.
Nécessite une amélioration	Les faiblesses relevées, prises individuellement ou collectivement, sont importantes et peuvent compromettre les objectifs de contrôle ou la bonne gestion de l’activité vérifiée.

Annexe C – Recommandations et réponse de la direction

Recommandation issue de la vérification	Réponse de la direction	Calendrier d'achèvement
1. Le directeur général, Direction générale de la technologie de l'information, de la gestion de l'information, de l'administration et de la protection des renseignements personnels, devrait mettre à jour la documentation définissant les exigences en matière de contrôle de l'accès ainsi que les procédures relatives à la création, à la modification et à la désactivation de l'accès au RPSC et au système Pension à vie pour les utilisateurs internes et externes.	La direction est d'accord avec cette recommandation. Nous réviserons et améliorerons notre documentation relative aux exigences et aux procédures afin d'y inclure des processus clairs pour la création, la modification et la désactivation de l'accès au RPSC et au système Pension à vie. Cet effort nécessitera la collaboration de la TI et des intervenants en matière du RPSC et du système Pension à vie afin de s'assurer que la documentation est conforme aux procédures organisationnelles et aux processus d'approbation. Ces mesures combleront les lacunes actuelles des procédures et de la documentation et renforceront une approche cohérente et sécuritaire de la gestion du contrôle de l'accès au RPSC et au système Pension à vie.	Décembre 2025
2. Le directeur général de la Gestion des programmes et de la prestation des services, en collaboration avec le directeur général de la Technologie de l'information, de la Gestion de l'information, de l'Administration et de la Protection des renseignements personnels, devrait définir et communiquer qui est responsable des matrices de contrôle d'accès pour le RPSC et le système Pension	La direction est d'accord avec cette recommandation. ACC a établi les rôles et les responsabilités liés aux systèmes destinés aux clients, tels que le RPSC et GCcas (Pension à vie). Nous tirerons parti de ces responsabilités existantes pour garantir l'attribution des responsabilités pour les matrices. ACC veillera à ce que la clarification et la communication des tâches précises soient assurées auprès de tous les intervenants et partenaires.	Mars 2026

à vie et ce que ces responsabilités impliquent.		
3. Le directeur général, Technologie de l'information, Gestion de l'information, Administration et Protection des renseignements personnels, devrait élaborer et mettre en œuvre un processus d'attribution des droits d'accès d'administrateur du système dans le système Pension à vie, examiner la liste des utilisateurs actuels qui ont des droits d'accès d'administrateur du système, supprimer les utilisateurs inutiles de ce rôle et ajouter le rôle à la matrice.	La direction est d'accord avec cette recommandation. Nous mettrons en place un processus pour demander, approuver et attribuer des privilèges élevés dans le système Pension à vie et veillerons à ce que toutes les parties concernées en soient informées. Nous procéderons à un examen des utilisateurs actuels disposant d'un accès d'administrateur du système et supprimerons les utilisateurs qui n'ont plus besoin de ce rôle, le cas échéant. Nous ajouterons le rôle d'administrateur du système à la matrice de contrôle d'accès.	Juin 2025
4. Le directeur général, Technologie de l'information, Gestion de l'information, Administration et Protection des renseignements personnels, devrait mettre en œuvre un processus visant à informer les utilisateurs autorisés de l'utilisation acceptable du RPSC et du système Pension à vie au moment où l'accès à ces systèmes leur est accordé ou modifié.	La direction est d'accord avec cette recommandation. Pour remédier à cela, nous inclurons une communication appropriée sur l'utilisation acceptable lorsque l'accès est accordé ou modifié. Ces efforts permettront de sensibiliser davantage les utilisateurs, de promouvoir la responsabilisation et d'atténuer les risques liés à une utilisation inacceptable.	Juin 2025
5. Le directeur général, Technologie de l'information, Gestion de l'information, Administration et Protection des renseignements personnels, devrait définir, documenter et mettre en œuvre un processus opérationnel pour l'examen périodique des comptes	La direction est d'accord avec cette recommandation. Pour remédier à cette situation, nous mettrons en place un processus d'examen cyclique dans le cadre duquel les autorités responsables de l'accès aux comptes du RPSC et du système Pension à vie examineront et confirmeront périodiquement que les niveaux d'accès restent appropriés.	Juin 2026

d’utilisateurs dans le RPSC et le système Pension à vie.		
6. Le directeur général, Technologie de l’information, Gestion de l’information, Administration et Protection des renseignements personnels, devrait définir, documenter et mettre en œuvre un processus opérationnel pour permettre de surveiller et d’analyser les activités des utilisateurs dans le RPSC et le système Pension à vie et de créer des rapports à cet égard.	La direction est d’accord avec cette recommandation. Un processus opérationnel sera élaboré pour surveiller régulièrement l’accès aux renseignements de nature délicate contenus dans le RPSC et le système Pension à vie. Le processus comprendra une enquête administrative appropriée et un suivi lorsque cela sera justifié. La formation et la sensibilisation feront également partie de la solution afin de renforcer l’importance du besoin de savoir tout en permettant aux utilisateurs d’exercer efficacement leurs fonctions.	Décembre 2025

Annexe D – Glossaire

Terme	Définition
Groupe opérationnel	La matrice du système Pension à vie répertorie environ 40 groupes opérationnels qui peuvent avoir accès au système en fonction du type de travail à effectuer (p. ex. APP – CTC, agents des services administratifs, gestionnaires de cas, etc.). Chaque groupe reçoit entre 1 et 5 rôles (rôles de sécurité) dans le système Pension à vie qui déterminent les éléments auxquels le système leur donne accès.
Réseau de prestation des services aux clients (RPSC)	Le Réseau de prestation des services aux clients (RPSC) est un système d'information utilisé par le personnel d'ACC pour faciliter la prestation de services aux clients, notamment en ce qui concerne les avantages pour les vétérans et la gestion de cas.
GCcas – Pension à vie	Un système d'information utilisé par le personnel d'ACC pour aider à verser la pension à vie aux clients qui vivent avec une invalidité attribuable à une blessure ou à une maladie liée au service.
Projet de modernisation de la TI	Un projet d'ACC qui vise à simplifier les systèmes de prestation de services aux clients afin de les rendre plus accessibles, plus conviviaux et plus faciles à entretenir.
Moindre privilège	Le concept consistant à limiter l'accès autorisé des utilisateurs selon les besoins, afin qu'ils puissent accomplir les tâches qui leur sont assignées.
Ancien système	Logiciels et/ou matériel informatique obsolètes qui sont toujours utilisés.
Matrice	Un outil utilisé pour définir et gérer les droits d'accès à divers systèmes, applications ou données. Il décrit les rôles autorisés à accéder à des ressources précises ou à prendre certaines mesures au sein d'un système. Il définit la relation entre les rôles et les autorisations ou niveaux d'accès qui leur sont attribués.
Tolérance au risque	La tolérance au risque désigne la volonté d'une organisation d'accepter ou de rejeter un certain niveau de risque résiduel. La tolérance au risque doit être clairement comprise par les personnes qui prennent des décisions liées au risque. Il faut que la tolérance au risque soit claire

	à tous les niveaux de l'organisation afin de favoriser une prise de décisions fondée sur l'analyse du risque et le recours à des approches qui tiennent compte du risque. Guide de gestion intégrée du risque – Canada.ca
Administrateur du système	Les utilisateurs qui ont généralement un accès beaucoup plus étendu aux systèmes que l'utilisateur moyen, car ils effectuent des tâches en arrière-plan telles que la programmation, l'attribution des droits d'accès, etc.
Répartition des tâches	La pratique consistant à répartir les responsabilités liées à des tâches connexes entre différentes personnes afin de réduire le risque d'erreurs, de fraudes ou de mesures inappropriées.
Description de travail	La matrice du RPSC répertorie des descriptions de travail sur environ 45 pages qui peuvent avoir accès au système en fonction du type de travail à effectuer (p. ex. agents des prestations d'invalidité, agents des services administratifs, gestionnaires de cas, etc.). Chaque groupe reçoit de nombreux niveaux d'accès (rôles de sécurité) qui déterminent les éléments auxquels le système leur donne accès.