Vérificateur général
MANITOBA

Rapport à l'Assemblée législative du Manitoba

Accès privilégiés aux systèmes d'information

Rapport d'audit indépendant

Version du site Web

octobre 2022

Cette page a été laissée
blanche intentionnellement.

La traduction de ce rapport a été fournie par le Service de traduction du Manitoba. En cas d'incohérence, se reporter à la version anglaise.

Cette page a été laissée
blanche intentionnellement.

Table des matières

Cette page a été laissée
blanche intentionnellement.

Commentaires du vérificateur général

Les systèmes d'information aident la Province du Manitoba (la Province) à offrir un éventail de services, notamment en matière de soins de santé, de possibilités d'inscription ou d'enregistrement en ligne, de demandes à des programmes provinciaux et du traitement de paiements. Ces systèmes renferment une grande quantité de renseignements personnels, du domaine de la santé et sur les entreprises, ce qui en fait des cibles pour les auteurs de cybermenaces.

La Province a recours à des utilisateurs privilégiés pour superviser ces systèmes d'information. Ceux-ci peuvent ajouter ou supprimer des utilisateurs, modifier des privilèges, changer les configurations des systèmes et les paramètres de sécurité et modifier les tables de données. Une personne possédant un accès privilégié non autorisé pourrait voler des données ou des fonds, perturber les opérations ou mettre le système en panne. Par conséquent, les normes gouvernementales exigent l'application de contrôles supplémentaires pour protéger les comptes d'accès privilégié.

Dans des rapports antérieurs publiés par mon Bureau, nous avons souligné des problèmes concernant la faiblesse du contrôle et le manque de surveillance des activités des utilisateurs privilégiés. Malheureusement, nous avons retrouvé ces mêmes problèmes lors de la préparation du présent rapport. Nous avons constaté que la Province ne contrôle pas les droits d'accès privilégiés suffisamment bien pour empêcher l'accès non autorisé aux systèmes d'information. Le présent rapport renferme cinq recommandations.

Étant donné la nature délicate de la cybersécurité, nous avons présenté des constatations plus détaillées et des recommandations supplémentaires dans des lettres internes à l'intention du ministère du Travail, de la Protection du consommateur et des Services gouvernementaux, ainsi que de Soins communs. Il est impératif que ces recommandations donnent lieu à la prise de mesures immédiates.

J'aimerais remercier les dirigeants et le personnel du ministère et de Soins communs, pour leur coopération et

Autres audits que nous avons menés en lien avec les contrôles de cybersécurité :

- Bureau de l'état civil, septembre 2020
- DossiÉ Manitoba, octobre 2018
- Gestion des risques associés aux appareils des utilisateurs finaux par l'Office régional de la santé de Winnipeg, juillet 2015

leur aide au cours de cet audit. J'aimerais également saluer les membres de mon équipe d'audit pour leur dévouement et leur travail rigoureux.

Tyson Shtykalo, CPA, CA
Vérificateur général

Points saillants du rapport

Raison pour laquelle nous avons mené cet audit

- La Province du Manitoba (la Province) s'appuie sur des systèmes d'information qui renferment des renseignements personnels, du domaine de la santé et sur les entreprises afin d'offrir divers services.
- Des contrôles appropriés sont nécessaires pour veiller à ce que seuls les utilisateurs autorisés disposent d'accès privilégiés à ces systèmes, leur permettant de modifier les privilèges des utilisateurs, de changer les configurations des systèmes et de modifier les paramètres de sécurité.
- Sans ces contrôles appropriés, il y a plus de risques que les auteurs de cybermenaces puissent obtenir un accès privilégié, entraînant des vols de données, des perturbations des opérations, des pannes de système et des pertes financières.

Objectif

Déterminer si l'utilisation de droits d'accès privilégiés est restreinte et contrôlée afin d'empêcher tout accès non autorisé aux systèmes d'information.

Conclusion

La Province ne contrôle pas les droits d'accès privilégiés suffisamment bien pour empêcher l'accès non autorisé aux systèmes d'information.

Notre rapport renferme 5 RECOMMANDATIONS.

Nos constatations

Les contrôles en place pour veiller à ce que des droits d'accès privilégiés soient accordés aux utilisateurs autorisés sont inadéquats.

- Les processus d'examen des droits d'accès privilégiés sont inadéquats.
- Les accès d'utilisateurs privilégiés non nécessaires ne sont pas retirés rapidement.
- Les approbations de droits d'accès privilégiés ne sont pas toujours documentées.

Les contrôles d'identification et d'authentification doivent être renforcés.

- Les normes qui régissent les mesures d'identification et d'authentification sont inadéquates.
- Les systèmes d'information ne sont pas configurés de façon à imposer des mots de passe de qualité.

La surveillance des activités des utilisateurs privilégiés est insuffisante.

- Les processus de journalisation et de surveillance des activités des utilisateurs privilégiés sont inexistants ou doivent être améliorés.
- Les activités à risque plus élevé ne sont pas toujours répertoriées en vue de leur surveillance.

Cette page a été laissée
blanche intentionnellement.

Contexte

La Province du Manitoba (la Province) a recours à des **systèmes d'information** qui l'aident à offrir une large gamme de services à la population. Cela comprend des soins de santé, des possibilités d'inscription ou d'enregistrement en ligne, des demandes à des programmes provinciaux et le traitement de paiements. Ces systèmes d'information renferment des quantités importantes de renseignements personnels, du domaine de la santé et sur les entreprises. Ils doivent être bien protégés afin d'éviter l'accès non autorisé à ces renseignements et de permettre d'y accéder selon les besoins.

Un **système d'information** s'entend d'un ensemble de plusieurs composants, notamment du matériel et des logiciels, participant à la collecte, au traitement, au stockage et à la diffusion de renseignements.

La Division des solutions numériques et technologiques (« Solutions numériques et technologiques », anciennement appelée « Technologie et transformation opérationnelle ») est l'organisme principal assumant la responsabilité générale de la stratégie, des politiques et de la prestation de services du gouvernement du Manitoba en ce qui a trait à la technologie de l'information et à la transformation opérationnelle. C'est une division du ministère du Travail, de la Protection du consommateur et des Services gouvernementaux. Solutions numériques et technologiques fournit du soutien à la plupart des ministères concernant leurs systèmes d'information. Les systèmes des soins de santé font exception. Ces derniers sont gérés par Soins communs, l'organisme de santé provincial qui coordonne la planification des soins axés sur les patients pour l'ensemble du Manitoba et qui offre des fonctions administratives et de gestion à tous les organismes de santé du Manitoba.

Les utilisateurs des systèmes d'information dotés d'un accès privilégié ont davantage de privilèges et de pouvoir que les utilisateurs généraux. Les organismes ont besoin que des utilisateurs privilégiés effectuent des activités comme ajouter ou supprimer des utilisateurs, modifier des privilèges, changer les configurations du système et les paramètres de sécurité et modifier les tables de données. On appelle également les utilisateurs privilégiés des administrateurs de système ou des superutilisateurs. Les systèmes d'information comprennent les applications opérationnelles, les **systèmes d'exploitation**, les **bases de données** et les infrastructures de réseau partagé comme les **pare-feu**. Les systèmes d'information ont souvent plusieurs utilisateurs privilégiés. Cela permet aux

Un **système d'exploitation** est un programme qui agit comme une interface entre le matériel informatique du système et l'utilisateur. On peut citer par exemple Microsoft Windows, macOS et Linux.

Une **base de données** est un ensemble de renseignements ou de données organisé selon une structure, habituellement stocké sous forme électronique dans un système informatique.

Un **pare-feu** est la partie d'un réseau informatique conçue pour bloquer les accès externes non autorisés, tout en permettant les communications sortantes depuis le réseau.

organismes de s'assurer qu'ils ne dépendent pas d'une seule personne. Pour satisfaire aux demandes opérationnelles, les utilisateurs privilégiés de Solutions numériques et technologiques et de Soins communs comprennent des employés du gouvernement et de fournisseurs.

Les organismes pourraient devoir affronter de graves répercussions si les **auteurs de cybermenaces** parviennent à obtenir un accès privilégié à leurs systèmes d'information. Ces répercussions peuvent comprendre des vols de données, des perturbations des opérations, des pannes de système et des pertes financières. Les auteurs de cybermenaces tentent d'obtenir un accès privilégié par différentes méthodes comme **l'hameçonnage**, **l'attaque par force brute** et **l'attaque par bourrage d'identifiants**. Ils ciblent en particulier les utilisateurs privilégiés dans le but de prendre le contrôle d'un système comme point de départ pour entrer dans d'autres systèmes de l'organisme.

Les organismes utilisent différents processus pour gérer les accès privilégiés, notamment la **fourniture d'accès,** l'**identification,** l'**authentification** et la **surveillance des activités.**

Les **auteurs de cybermenaces** sont les États, les groupes ou les personnes qui, dans l'intention de nuire, cherchent à tirer avantage des vulnérabilités, d'une sensibilisation insuffisante à la cybersécurité ou de progrès technologiques pour obtenir un accès non autorisé à des systèmes d'information ou encore porter préjudice aux données, aux dispositifs, aux systèmes et aux réseaux des victimes.

L'**hameçonnage** est une technique dans laquelle un attaquant trompe une personne grâce à des courriels ou à des messages textes pour lui faire révéler des renseignements sensibles ou déployer un logiciel malveillant sur son système d'information.

L'**attaque par force brute** consiste à tenter de trouver le mot de passe d'un utilisateur en procédant à des essais répétés.

L'**attaque par bourrage d'identifiants** consiste à obtenir une liste de données d'accès, comme des mots de passe, et à l'utiliser dans de nombreuses tentatives de connexion à divers comptes.

La **fourniture d'accès** est le processus par lequel les utilisateurs obtiennent un accès leur permettant d'exercer leurs fonctions et leurs responsabilités.

L'**identification** est le processus servant à établir et à prouver l'identité d'une personne. L'authentification est le processus de vérification de l'identité d'un utilisateur qui demande l'accès.

La **surveillance des activités** est l'examen régulier des activités effectuées par les utilisateurs privilégiés afin de déceler les comportements suspects ou les risques à la sécurité des systèmes d'information.

Objectif de l'audit

Nous visions à déterminer si l'utilisation de droits d'accès privilégiés est restreinte et contrôlée afin d'éviter l'accès non autorisé aux systèmes d'information.

Portée et approche

L'audit comprenait un examen de documents, de procédures, de normes, de rapports, de paramètres système et d'autres renseignements relatifs aux processus de gestion des utilisateurs privilégiés des systèmes d'information gérés par Solutions numériques et technologiques du ministère du Travail, de la Protection du consommateur et des Services gouvernementaux, ainsi que par Soins communs.

Nous avons eu des entretiens avec des intervenants et des responsables de processus clés de systèmes d'information afin de comprendre les contrôles utilisés pour limiter l'utilisation des droits d'accès des utilisateurs privilégiés et empêcher les accès non autorisés.

Nous avons testé des échantillons de différentes tailles pour évaluer l'efficacité des contrôles sur la gestion des accès privilégiés. Nous avons choisi des échantillons provenant de systèmes clés renfermant des renseignements personnels, du domaine de la santé et sur les entreprises de nature sensible et comprenant des **comptes** individuels, de **service** et de **système**.

Le présent audit n'a pas vérifié la mauvaise utilisation d'accès privilégiés.

Un **compte système** est un compte par défaut qui est créé avec le système.

Un **compte de service** est utilisé par un système d'information pour exécuter des services et des processus internes automatisés.

Critères d'audit

Pour effectuer le présent audit, nous avons utilisé les critères suivants :

	Critères	Sources
1.1	Des contrôles devraient être en place pour garantir que les droits d'accès privilégiés sont accordés à des utilisateurs autorisés.	COSO, contrôle 10 ISO/IEC 27002, contrôles 7.1, 9.1 et 9.2 CIS, contrôle 6
1.2	Des contrôles d'identification et d'authentification devraient être en place pour garantir que seuls les utilisateurs privilégiés autorisés peuvent accéder aux systèmes.	ISO/IEC 27002, contrôles 9.4.2 et 9.4.3 CIS, contrôle 6
1.3	Les activités des utilisateurs privilégiés devraient être surveillées afin de détecter les activités non autorisées.	ISO/IEC 27002, contrôle 12.4 CIS, contrôle 6

Cette page a été laissée
blanche intentionnellement.

La Province ne contrôle pas les droits d'accès privilégiés suffisamment bien pour empêcher l'accès non autorisé aux systèmes d'information

Le ministère du Travail, de la Protection du consommateur et des Services gouvernementaux ainsi que Soins communs ont mis en œuvre des politiques et des procédures pour gérer les accès privilégiés et protéger leurs systèmes d'information. Cependant, nous avons conclu que les contrôles des accès privilégiés en place n'étaient pas appropriés pour empêcher et détecter les accès non autorisés aux systèmes d'information. Notre conclusion s'appuie sur les constatations suivantes :

- Les contrôles visant à s'assurer que les droits d'accès privilégiés sont accordés à des utilisateurs autorisés sont inadéquats **(SECTION 1)**.
- Les contrôles d'identification et d'authentification doivent être renforcés **(SECTION 2)**.
- La surveillance des activités des utilisateurs privilégiés est insuffisante **(SECTION 3)**.

Étant donné la nature délicate des constations sur la sécurité, nous avons présenté nos observations plus détaillées et nos recommandations dans des lettres internes à l'intention du ministère du Travail, de la Protection du consommateur et des Services gouvernementaux, ainsi que de Soins communs. Si cette information était divulguée au grand public, les auteurs de cybermenaces pourraient s'en servir pour compromettre la sécurité des systèmes exploités par ces entités.

1 Les contrôles visant à s'assurer que les droits d'accès privilégiés sont accordés à des utilisateurs autorisés sont inadéquats

Des contrôles doivent être en place pour veiller à ce que des droits d'accès aux systèmes d'information soient accordés seulement aux utilisateurs autorisés. Ces contrôles aident à préserver la confidentialité, l'intégrité et la disponibilité des systèmes.

Dans le cadre de leurs processus de recrutement, le ministère du Travail, de la Protection du consommateur et des Services gouvernementaux ainsi que Soins communs (les entités) exigent que les employés passent des vérifications de sécurité. Pour empêcher les accès non autorisés, il est important que les accès des utilisateurs aux actifs soient approuvés, et que la documentation étayant ces approbations soit conservée en vue de consultations ultérieures. Ces droits d'accès doivent être examinés périodiquement pour s'assurer qu'ils correspondent aux responsabilités des postes en question. Les accès qui ne sont pas nécessaires devraient être retirés rapidement.

Nous avons constaté que les contrôles mis en œuvre par les entités pour s'assurer que les utilisateurs privilégiés sont autorisés et qu'ils ont des droits d'accès appropriés sont inadéquats. Notre conclusion s'appuie sur les constatations suivantes :

- Soins communs ne conserve pas toujours la documentation étayant les approbations accordant des droits d'accès privilégiés **(SECTION 1.1)**.
- Les accès d'utilisateurs privilégiés non nécessaires ne sont pas retirés rapidement **(SECTION 1.2)**.
- Les processus d'examen des accès privilégiés sont inadéquats **(SECTION 1.3)**.

1.1 Soins communs ne conservait pas toujours la documentation étayant les approbations accordant des droits d'accès privilégiés

La norme relative aux comptes d'administration en matière de *technologie de l'information et des communications* (TIC) *de Soins communs* exige que des comptes privilégiés ne soient créés que lorsqu'une demande d'approbation a été soumise au bureau de service.

Nous n'avons trouvé aucune documentation se rapportant aux approbations de droits d'accès privilégiés pour certains utilisateurs figurant dans l'échantillon de Soins commun. Nous avons obtenu des responsables de l'entité la confirmation que ces utilisateurs devaient avoir ces accès pour exercer leurs fonctions. L'absence de documentation relative à ces approbations entraîne le risque d'accorder à des personnes un accès non approprié aux systèmes d'information et aux données.

En outre, nous avons constaté que, pour plusieurs des applications que nous avons sélectionnées pour les vérifier, Soins communs n'avait pas désigné les responsables chargés d'approuver l'accès à celles-ci. En l'absence d'une liste documentée et approuvée de personnes autorisées à approuver cet accès, il existe un risque que des accès non appropriés aux systèmes de Soins communs soient accordés. Une liste d'approbateurs est utilisée par le personnel qui gère les accès aux applications afin de confirmer qu'un approbateur de demande d'accès a le pouvoir d'autoriser un accès. Les responsables de Soins communs ont reconnu le manque de procédure officielle et confirmé que toutes les demandes d'accès étaient autorisées.

Recommandation 1

Nous recommandons que Soins communs :

- prépare une liste de responsables autorisés qui seront chargés d'approuver les demandes d'accès aux applications;
- accorde les accès seulement après avoir validé l'approbation de ces responsables autorisés;
- conserve les documents étayant les approbations d'accès.

1.2 Les accès d'utilisateurs privilégiés non nécessaires ne sont pas retirés rapidement

Les normes des entités exigent que les accès des utilisateurs ayant cessé leurs fonctions soient retirés rapidement. Nous avons examiné un échantillon d'utilisateurs privilégiés qui avaient quitté les entités faisant l'objet de l'audit. Nous avons constaté que les accès de la plupart de ces utilisateurs n'avaient pas été retirés rapidement. Ce problème était présent dans l'ensemble des applications et des systèmes d'infrastructures gérés par les entités.

Les processus que les entités utilisent reposent sur la présentation, par les gestionnaires et les superviseurs, de demandes de retrait des accès. Comme les gens ont naturellement tendance à oublier les choses, il existe un risque que les gestionnaires et les superviseurs ne présentent pas ces demandes. Les entités peuvent retirer rapidement les accès en intégrant des processus de retrait des accès aux processus de ressources humaines et en mettant en œuvre des flux opérationnels automatisés.

Recommandation 2

Nous recommandons que le ministère du Travail, de la Protection du consommateur et des Services gouvernementaux, ainsi que Soins communs :

- recherchent et mettent en œuvre des solutions automatisées afin d'améliorer la gestion des accès privilégiés;
- intègrent aux ressources humaines des processus de retrait des accès, afin de retirer rapidement les autorisations des utilisateurs.

1.3 Processus d'examen des droits d'accès privilégiés inadéquats

La *norme relative au contrôle des accès du Manitoba* et la *norme relative aux comptes d'administration en matière de TIC de Soins communs* exigent que les utilisateurs soient vérifiés périodiquement pour s'assurer que leurs privilèges d'accès sont appropriés et confirmer que les accès des personnes qui ont changé de poste ou ont quitté ces entités ont été retirés.

Nous avons constaté que les droits d'accès des utilisateurs privilégiés n'étaient pas examinés pour la plupart des systèmes que nous avons sélectionnés pour les vérifier. Dans quelques cas, ces examens étaient effectués, mais pas en temps opportun.

Nous avons aussi passé en revue certains utilisateurs privilégiés pour déterminer si leurs accès privilégiés étaient nécessaires. Nous avons constaté que plusieurs utilisateurs disposaient d'accès qui ne leur étaient pas nécessaires et n'avaient pas été retirés. Effectuer des examens réguliers des utilisateurs privilégiés et de leurs droits d'accès garantit que les accès demeurent appropriés et que les accès non nécessaires sont retirés rapidement.

Recommandation 3

Nous recommandons que le ministère du Travail, de la Protection du consommateur et des Services gouvernementaux, ainsi que Soins communs :

- procèdent régulièrement à l'examen des utilisateurs privilégiés de tous les systèmes d'information pour vérifier que leurs droits d'accès correspondent aux responsabilités de leur poste et garantir qu'aucun privilège d'accès non autorisé n'est accordé;
- retirent les droits d'accès non nécessaires rapidement après cet examen;
- conservent les documents étayant ces examens des droits d'accès.

2 Les contrôles d'identification et d'authentification doivent être renforcés

Les contrôles d'identification et d'authentification sont fondamentaux pour restreindre l'accès aux données et aux systèmes d'information. Ces contrôles aident à s'assurer que les utilisateurs sont bien qui ils disent être, et qu'ils disposent des accès appropriés aux systèmes et aux données.

Nous avons constaté des faiblesses dans les contrôles d'identification et d'authentification utilisés par les entités pour veiller à ce que seuls les utilisateurs privilégiés autorisés puissent accéder aux systèmes.

2.1 Les contrôles d'identification et d'authentification doivent être améliorés

Nous avons testé un échantillon de systèmes d'information et constaté que les contrôles d'identification et d'authentification des utilisateurs privilégiés doivent être renforcés. Par exemple, des améliorations doivent être apportées aux normes qui régissent l'identification et l'authentification, et les systèmes d'information n'ont pas été configurés de façon à imposer des mots de passe de qualité, comme l'exigent les normes connexes du Manitoba et de Soins communs.

Le respect de normes rigoureuses aide à empêcher les accès non autorisés aux systèmes d'information. De bonnes normes d'identification et d'authentification comprennent l'authentification multifacteur, un nombre maximum de tentatives de connexion échouées, une déconnexion des sessions inactives, une longueur minimum de mot de passe, des critères de complexité du mot de passe (majuscule, minuscule, chiffre, caractères spéciaux), une durée de vie du mot de passe et un historique des mots de passe (nombre de mots de passe précédents que le système garde en mémoire).

Étant donné la nature délicate des constatations sur la sécurité, nous avons présenté nos constatations et nos recommandations plus détaillées dans des lettres internes à l'intention des entités.

Recommandation 4

Nous recommandons que le ministère du Travail, de la Protection du consommateur et des Services gouvernementaux ainsi que Soins communs mettent en œuvre les normes d'identification et d'authentification ainsi que les recommandations en matière de contrôles présentées dans nos lettres aux dirigeants.

3 Surveillance inadéquate des activités des utilisateurs privilégiés

Surveiller les activités des utilisateurs privilégiés est important, car cela aide à détecter en temps opportun les mauvaises utilisations accidentelles ou malveillantes des accès privilégiés. Une détection rapide des activités malveillantes ou inappropriées permet d'y apporter une réponse en temps opportun et peut réduire les répercussions comme le vol de données et les pannes de système. Des exemples d'activités des utilisateurs privilégiés que les entités pourraient surveiller et journaliser sont des modifications inappropriées des systèmes ou des données, des changements apportés aux groupes d'utilisateurs privilégiés et des transactions effectuées avec des identifiants privilégiés.

Nous avons constaté que le ministère du Travail, de la Protection du consommateur et des Services gouvernementaux ainsi que Soins communs ne surveillaient et ne journalisaient pas les accès privilégiés de façon appropriée afin de détecter les activités interdites.

3.1 Manque de surveillance et de journalisation des activités des utilisateurs privilégiés

La *norme relative au contrôle des accès du Manitoba* exige que les utilisateurs dotés d'accès privilégiés soient soumis à des contrôles supplémentaires. Ceux-ci comprennent la journalisation des audits supplémentaires et l'examen de l'utilisation des accès privilégiés.

La Politique sur les technologies de l'*information et des communications de Soins communs* relative à la journalisation et la surveillance exige que la direction surveille les systèmes d'information pour détecter les violations de sécurité grâce à une piste d'audit automatisé des événements de sécurité.

Un mauvais usage des accès privilégiés pourrait entraîner de graves répercussions. En conséquence, il est important de journaliser toutes les activités des utilisateurs privilégiés et d'examiner celles susceptibles d'indiquer un événement de sécurité, qui pourrait constituer une activité inappropriée ou anormale. Les journaux sont aussi précieux pour enquêter sur les activités illicites et pourraient être requis pour respecter la législation.

Pour la plupart des systèmes que nous avons testés, nous avons constaté soit l'absence de processus en place pour surveiller et journaliser les activités des utilisateurs privilégiés, soit la nécessité d'améliorer

ces processus. Par exemple, nous avons noté des cas où les entités n'avaient pas déterminé les activités des utilisateurs privilégiés devant être surveillées. Déterminer les activités à surveiller aiderait les entités à concentrer leurs efforts de surveillance sur les événements les plus pertinents, comme ceux qui présentent le risque le plus élevé de représenter une violation des systèmes. Nous avons aussi noté que les activités exercées avec l'identifiant de certains utilisateurs privilégiés n'étaient pas surveillées ni journalisées.

Nous avons noté que le recours à des procédures manuelles pour surveiller les activités prend naturellement beaucoup de temps et est sujet à des erreurs en raison de la quantité d'événements journalisés. Cela peut entraîner des retards dans la détection d'événements de sécurité ou à des absences de détection. Les outils de journalisation automatisée aident à regrouper et à prioriser la surveillance des événements à risque.

Recommandation 5

Nous recommandons que le ministère du Travail, de la Protection du consommateur et des Services gouvernementaux, ainsi que Soins communs :

- journalisent toutes les activités des utilisateurs privilégiés;
- déterminent les activités à risque et les examinent régulièrement;
- cherchent des méthodes, lorsqu'il n'y en a pas déjà en œuvre, afin d'automatiser la surveillance des utilisateurs privilégiés, notamment la mise en place d'alertes d'activités à examiner.

Renseignements supplémentaires sur l'audit

Ce rapport de certification indépendant sur les accès privilégiés a été préparé par le Bureau du vérificateur général du Manitoba. Nous avions la responsabilité de fournir des renseignements objectifs, des conseils et une certification en vue d'aider l'Assemblée législative à surveiller la gestion des ressources et des programmes par le gouvernement et de déterminer si l'utilisation de droits d'accès privilégiés est restreinte et contrôlée afin d'empêcher l'accès non autorisé aux systèmes d'information.

Tout le travail de cet audit a été exécuté à un niveau de certification raisonnable, conformément à la Norme canadienne de missions de certification (NCMC) 3001 – Missions d'appréciation directe établie par les Comptables professionnels agréés du Canada (CPA Canada) dans le Manuel de CPA Canada – Certification.

Le Bureau applique la Norme canadienne de contrôle qualité (NCCQ) 1 et, par conséquent, assure un système exhaustif de contrôle de la qualité, y compris des politiques et des procédures documentées concernant la conformité avec les règles de déontologie, les normes professionnelles et les exigences législatives et réglementaires applicables.

Pour effectuer notre travail d'audit, nous avons respecté les normes d'indépendance et les autres règles déontologiques du code de conduite professionnelle de l'Ordre des comptables professionnels agréés du Manitoba et le Code de valeurs, d'éthique et de conduite professionnelle du Bureau du vérificateur général du Manitoba. Tant les règles du code de conduite de l'Ordre des comptables que le Code du Bureau du vérificateur général se fondent sur des principes fondamentaux d'intégrité, d'objectivité, de professionnalisme, de compétence et de diligence professionnelles, de confidentialité et de comportement professionnel.

Conformément à notre processus d'audit habituel, nous avons obtenu ce qui suit de la part de la direction :

1. la confirmation de la responsabilité de la direction quant à l'objet de l'audit;
2. la reconnaissance de la pertinence des critères utilisés pour l'audit;
3. la confirmation que tous les renseignements connus qui ont été demandés ou qui pourraient avoir une incidence sur les constatations ou la conclusion de l'audit ont été fournis.

Période couverte par l'audit

L'audit concernait la période allant de janvier 2018 à mars 2022, période à laquelle la conclusion de l'audit s'applique. Néanmoins, pour mieux comprendre l'objet de l'audit, nous nous sommes également penchés sur certains points qui ont précédé et suivi la période couverte par l'audit.

Date du rapport d'audit

Nous avons obtenu des éléments de preuve d'audit suffisants et appropriés sur lesquels fonder notre conclusion le 12 août 2022, à Winnipeg (Manitoba).

Cette page a été laissée
blanche intentionnellement.

Résumé des recommandations et des réponses des responsables

RECOMMANDATION 1

Nous recommandons que Soins communs :

- prépare une liste de responsables autorisés qui seront chargés d'approuver les demandes d'accès aux applications;
- accorde les accès seulement après avoir validé l'approbation de ces responsables autorisés;
- conserve les documents étayant les approbations d'accès.

Réponse de Soins communs :

Soins communs a en place de bonnes pratiques en ce qui concerne les demandes d'accès (qu'il s'agisse d'un accès ordinaire ou privilégié) aux systèmes et aux applications que nous gérons. Nous prenons acte des exceptions à nos bonnes pratiques qui ont été relevées dans le cadre de l'audit et explorerons les possibilités de mettre ces exceptions en conformité avec nos bonnes pratiques.

RECOMMANDATION 2

Nous recommandons que le ministère du Travail, de la Protection du consommateur et des Services gouvernementaux, ainsi que Soins communs :

- recherchent et mettent en œuvre des solutions automatisées afin d'améliorer la gestion des accès privilégiés;
- intègrent aux ressources humaines des processus de retrait des accès, afin de retirer rapidement les autorisations des utilisateurs.

Réponses des responsables :

Ministère du Travail, de la Protection du consommateur et des Services gouvernementaux : Le ministère du Travail, de la Protection du consommateur et des Services gouvernementaux est d'accord sur le fait que les accès des utilisateurs privilégiés devraient être retirés rapidement lorsque l'accès n'est plus requis. La direction a pris des mesures immédiates pour auditer les accès des utilisateurs privilégiés existants et élabore actuellement un plan pour retirer les accès non nécessaires. Afin d'atténuer les risques futurs et actuels, nous utiliserons une combinaison d'outils et d'améliorations des processus dans le cadre du programme de réduction des risques en matière de cybersécurité. L'enquête comprendra

une évaluation du niveau d'intégration requis avec les processus des ressources humaines, mais nous comprenons que des mesures supplémentaires s'imposent en plus de l'intégration, car des modifications des accès privilégiés seront dans certains cas nécessaires alors même qu'aucune activité (processus) correspondante des ressources humaines n'est prévue.

Soins communs :
Soins communs estime que le retrait opportun de l'accès est une partie importante de ses pratiques en matière de gestion de l'identité et de l'accès.

Nous avons pris acte des exceptions à nos pratiques actuelles et explorerons les possibilités de les mettre en conformité, notamment en améliorant la documentation qui justifie le maintien de l'accès après des modifications apportées au rôle de soutien d'une personne (p. ex., maintenir l'accès pour soutenir la technologie ancienne ou spécialisée).

Des fonds supplémentaires pourraient être nécessaires à l'acquisition des ressources, tant humaines que technologiques, qui seront requises pour satisfaire pleinement les exigences découlant de cette recommandation.

RECOMMANDATION 3

Nous recommandons que le ministère du Travail, de la Protection du consommateur et des Services gouvernementaux, ainsi que Soins communs :

- procèdent régulièrement à l'examen des utilisateurs privilégiés de tous les systèmes d'information pour vérifier que leurs droits d'accès correspondent aux responsabilités de leur poste et garantir qu'aucun privilège d'accès non autorisé n'est accordé;
- retirent les droits d'accès non nécessaires rapidement après cet examen;
- conservent les documents étayant ces examens des droits d'accès.

Réponses des responsables :

Ministère du Travail, de la Protection du consommateur et des Services gouvernementaux :
Le processus actualisé de gestion du risque et de la sécurité relatif aux TIC du ministère du Travail, de la Protection du consommateur et des Services gouvernementaux inclura des audits réguliers visant à vérifier si l'accès est requis et à prendre rapidement des mesures lorsque cela est jugé nécessaire. Toutefois, nous exigerons des ministères qu'ils vérifient les niveaux d'accès requis pour leur personnel et dans les cas où des systèmes ou applications sont gérés par les ministères ou leur appartiennent.

À l'avenir, nous collaborerons également avec Soins communs pour harmoniser les pratiques de sécurité au besoin.

Soins communs :
Soins communs estime que l'examen régulier des droits d'accès est un volet important de ses pratiques de gestion de l'identité et de l'accès. Nous acceptons la rétroaction concernant nos pratiques fournie dans les constatations de l'audit et les améliorations possibles définies dans la recommandation. Nous explorerons les possibilités de perfectionner notre pratique d'examen des droits d'accès privilégiés, y compris la documentation pertinente des examens.

Des fonds supplémentaires pourraient être nécessaires à l'acquisition des ressources, tant humaines que technologiques, qui seront requises pour satisfaire pleinement les exigences découlant de cette recommandation.

RECOMMANDATION 4

Nous recommandons que le ministère du Travail, de la Protection du consommateur et des Services gouvernementaux ainsi que Soins communs mettent en œuvre les normes d'identification et d'authentification ainsi que les recommandations en matière de contrôles présentées dans nos lettres aux dirigeants.

Réponses des responsables :

Ministère du Travail, de la Protection du consommateur et des Services gouvernementaux :
Le ministère du Travail, de la Protection du consommateur et des Services gouvernementaux adhère à cette recommandation dans son principe, tout en remarquant qu'une approche de portée générale n'est pas toujours pertinente. Les contraintes technologiques, le contenu de l'information, des systèmes et des applications et l'architecture des systèmes et des applications sont des considérations qui influent sur les contrôles nécessaires. Les recommandations du Bureau du vérificateur général seront prises en compte pour les ajouts ou les modifications à apporter aux contrôles et aux politiques dans le cadre du programme de réduction des risques en matière de cybersécurité.

À l'avenir, nous collaborerons également avec Soins communs pour harmoniser les pratiques de sécurité au besoin.

Soins communs :
Soins communs prend acte des constatations et des recommandations présentées dans la lettre à la direction. Des travaux sont en cours pour donner suite à certaines des recommandations, et Soins communs explorera les possibilités de satisfaire les exigences découlant de la recommandation qui pourraient nécessiter des ressources supplémentaires.

Cet audit était centré sur les pratiques et les contrôles de gestion des accès privilégiés de

l'ancien environnement du Programme de cybersanté du Manitoba, l'un des programmes de technologie de l'information (TI) qui soutenaient le système provincial de soins de santé. L'amorce de l'audit en 2019 a coïncidé avec l'établissement de Santé numérique sous l'égide de Soins communs – le fournisseur de services de TI de Soins communs – en avril 2019 par la fusion de divers programmes régionaux de TI ayant chacun, entre autres, ses pratiques, ses infrastructures et son personnel. Même si les recommandations sont centrées sur un ancien programme régional de TI, les réponses aux recommandations doivent prendre en compte la normalisation d'un programme provincial de TI dont la mise en œuvre et la gestion exigent des fonds et des ressources supplémentaires.

RECOMMANDATION 5

Nous recommandons que le ministère du Travail, de la Protection du consommateur et des Services gouvernementaux, ainsi que Soins communs :

- journalisent toutes les activités des utilisateurs privilégiés;
- déterminent les activités à risque et les examinent régulièrement;
- cherchent des méthodes, lorsqu'il n'y en a pas déjà en œuvre, afin d'automatiser la surveillance des utilisateurs privilégiés, notamment la mise en place d'alertes d'activités à examiner.

Réponses des responsables :

Ministère du Travail, de la Protection du consommateur et des Services gouvernementaux :
Le ministère du Travail, de la Protection du consommateur et des Services gouvernementaux adhère à cette recommandation dans son principe, tout en remarquant qu'une approche de portée générale n'est pas toujours pertinente. Les contraintes technologiques, le contenu de l'information, des systèmes et des applications et l'architecture des systèmes et des applications sont des considérations qui influent sur les contrôles nécessaires. Les recommandations du Bureau du vérificateur général seront prises en compte pour les ajouts ou les modifications à apporter aux contrôles et aux politiques dans le cadre du programme de gestion du risque et de la sécurité relatif aux TIC.

À l'avenir, nous collaborerons également avec Soins communs pour harmoniser les pratiques de sécurité au besoin.

Soins communs :
Soins communs est d'accord sur le fait que la surveillance des accès privilégiés est un contrôle important en matière de cybersécurité, et nous évaluerons dans quelle mesure certaines de nos nouvelles capacités de contrôle de la sécurité répondront à cette recommandation.

Cet audit était centré sur les pratiques et les contrôles de gestion des accès privilégiés de l'ancien environnement du Programme de cybersanté du Manitoba, l'un des programmes de technologie de l'information (TI) qui soutenaient le système provincial de soins de santé. L'amorce de l'audit en 2019 a coïncidé avec l'établissement de Santé numérique sous l'égide de Soins communs – le fournisseur de services de TI de Soins communs – en avril 2019 par la fusion de divers programmes régionaux de TI ayant chacun, entre autres, ses pratiques, ses infrastructures et son personnel. Même si les recommandations sont centrées sur un ancien programme régional de TI, les réponses aux recommandations doivent prendre en compte la normalisation d'un programme de TI provincial dont la mise en œuvre et l'entretien exigent des fonds et des ressources supplémentaires.

Notre vision
Être appréciés pour notre influence positive sur la performance du secteur public au moyen de travaux et de rapports d'audit aux effets importants.

Notre mission
Porter notre attention sur des domaines d'importance stratégique pour l'Assemblée législative et fournir aux députés de l'Assemblée des audits fiables et efficients.

Notre mission comprend la production de rapports d'audit faciles à comprendre qui incluent des discussions sur les bonnes pratiques au sein des entités verifiees et des recommandations que, une fois mises en œuvre auront des effets importants sur la performance du gouvernement.

Nos valeurs | Responsabilité | Intégrité | Confiance | Collaboration | Innovation | Croissance professionnelle

Vérificateur général
Tyson Shtykalo

Directeur général d'audits de technologies de l'information et de l'innovation
Wade Bo-Maguire

Responsable de l'audit informatique
Ganesh Sharma

Gestionnaire des communications
Frank Landry

Soutien administratif
Jomay Amora-Dueck
Tara MacKay

Conception graphique
Waterloo Design House

Version du site Web

Vérificateur général
MANITOBA

Pour plus de renseignements, veuillez communiquer avec notre bureau :

Bureau du vérificateur général
330, avenue Portage, bureau 500
Winnipeg (Manitoba) R3C 0C4

Téléphone : 204 945-3790 Télécopieur : 204 945-2169
contact@oag.mb.ca | www.oag.mb.ca

Facebook.com/AuditorGenMB
Twitter.com/AuditorGenMB
Linkedin.com/company/manitoba-auditor-general