Suivi de l'audit de l'optimisation des ressources de 2022

Ministère des Services au public et aux entreprises et de l'Approvisionnement

Bureau du directeur général de l'information pour la fonction publique

// Conclusion générale

43 recommandations

37 % (16)
Pleinement mise en œuvre

56 % (24)
En voie de mise en œuvre

7 % (3)
Peu ou pas de progrès

Le 20 août 2024, le ministère des Services au public et aux entreprises et de l'Approvisionnement avait pleinement mis en œuvre 37 % des mesures que nous avions recommandées dans notre audit de 2022 du **Bureau du directeur général de l'information pour la fonction publique**. Le Ministère a fait des progrès dans la mise en œuvre de 56 % des mesures recommandées.

Le Ministère a pleinement mis en œuvre des recommandations comme l'acquisition d'un fournisseur de réseau secondaire de secours pour ses activités de TI essentielles, en s'assurant qu'au moins deux candidats par poste de consultant en TI sont interviewés par au moins trois évaluateurs et la réévaluation de ses cibles de conformité pour s'assurer qu'elles correspondent aux normes de l'industrie.

Le Ministère a fait des progrès dans la mise en œuvre de recommandations comme renforcer les groupements de TI afin de respecter la norme de sécurité requise consistant à appliquer des contrôles de cybersécurité robustes, comme le chiffrement, et offrir des cours obligatoires de formation en cybersécurité à tout le personnel de la FPO, y compris les employés contractuels.

Toutefois, le Ministère a fait peu de progrès dans le cas de 7 % des recommandations, Par exemple dans l'évaluation visant à déterminer si tous les systèmes de TI nécessitent un plan de reprise après

sinistre de façon continue, et dans l'examen et l'évaluation de la conformité des groupements aux plans de reprise après sinistre au moins une fois par année et chaque fois qu'un changement important est apporté à l'environnement de TI de la FPO.

L'état des mesures prises en réponse à chacune de nos recommandations est exposé ci-après (de plus amples renseignements sont présentés à l'**annexe**).

// État des mesures prises en réponse aux recommandations

Nous avons effectué des travaux d'assurance entre mars 2024 et août 2024. Nous avons obtenu du ministère des Services au public et aux entreprises et de l'Approvisionnement des déclarations écrites selon lesquelles, au 15 octobre 2024, il nous avait fourni une mise à jour complète de l'état des recommandations que nous avions formulées à l'origine dans notre audit, il y a deux ans.

1. La structure hiérarchique empêche le Bureau du DGIFP de s'assurer que les groupements disposent de systèmes de TI offrant une exécution efficace et efficiente

Lors de notre audit, nous avons constaté que les groupements de services de TI relèvent de leurs sous-ministres respectifs et non du Bureau du directeur général de l'information pour la fonction publique (Bureau du DGIFP). Par conséquent, le Bureau du DGIFP n'est pas toujours au courant des décisions clés en matière de TI qui touchent l'approvisionnement d'une valeur inférieure à deux millions de dollars ou la protection des données de la population ontarienne recueillies par les groupements ni ne peut mesurer les résultats en matière de rendement des systèmes des groupements de services de TI.

Recommandation 1 : Mesures 1 et 2

Pour assurer une harmonisation claire des opérations entre les groupements de TI et pour que le Bureau du directeur général de l'information pour la fonction publique (Bureau du DGIFP) puisse surveiller et faire respecter adéquatement la reddition de comptes sur les opérations quotidiennes de TI afin que les groupements de TI exécutent leurs systèmes de TI de manière efficace et efficiente, le Secrétariat du Conseil du Trésor :

- collaborer avec les groupements de TI et leurs ministères respectifs afin que le niveau approprié de gouvernance, de surveillance et de responsabilisation soit en place;

- réévaluer les critères d'examen des systèmes de TI en fonction de l'impact et du risque plutôt que du seuil financier actuel de deux millions de dollars.

État : En voie de mise en œuvre d'ici janvier 2025.

Détails

Nous avons constaté qu'en avril 2023, le Bureau du DGIFP a redéfini les responsabilités professionnelles des dirigeants principaux de l'information (DPI) des groupements de TI au moyen d'un modèle de compétences. Ces nouvelles compétences exigent notamment que les DPI cernent les possibilités de collaboration interministérielle, comme l'échange de fiches d'évaluation du rendement pour les fournisseurs de TI afin de faciliter les approvisionnements futurs. De plus, tout au long de 2024, le Secrétariat du Conseil du Trésor (SCT), en collaboration avec les partenaires de TI, a poursuivi les travaux visant à actualiser la politique sur la passerelle des projets de TI, y compris la mise à jour du processus d'examen des projets de TI en fonction de l'incidence et des risques. Ce processus d'examen mis à jour nécessite l'apport et la communication des partenaires de TI, dont le Bureau du DGIFP, des groupements de TI et du groupe de l'architecture ministérielle et redéfinit les rôles et les responsabilités de chacun. La politique actualisée est en attente de sa présentation au Conseil du Trésor et au Conseil de gestion du gouvernement et de son approbation d'ici janvier 2025.

Nous avons examiné les commentaires que le SCT avait reçu des groupements au sujet de l'actualisation des politiques et constaté que des critères comme l'importance du projet ou le risque global seront pris en compte au seuil de deux millions de dollars (risque financier) en coûts estimatifs des projets. La politique prévoit également une orientation pour les projets évalués à moins de deux millions de dollars.

2. Le Bureau du DGIFP ne dresse pas de liste des risques en matière de TI au sein de la fonction publique de l'Ontario et ne relève pas non plus les risques en matière de TI au sein du Bureau du DGIFP

Lors de notre audit initial, nous avions constaté que le Bureau du DGIFPI ne disposait pas d'une stratégie globale à l'échelle de la FPO pour cerner les risques organisationnels en matière de TI et mettre en œuvre des stratégies d'atténuation et de correction.

Recommandation 2 : Mesures 1 et 2

Pour que les risques liés aux TI pour la fonction publique de l'Ontario (FPO) soient cernés, signalés et atténués de façon appropriée, le Bureau du directeur général de l'information pour la fonction publique devrait collaborer avec le Bureau du directeur général de la gestion des risques pour :

- élaborer et mettre en œuvre une stratégie globale qui englobe tous les risques en matière de TI qui touchent la FPO;
- mettre en place des mesures pour atténuer les risques de TI qui ont une incidence sur les opérations à l'échelle de la FPO;

État : En voie de mise en œuvre d'ici mars 2025.

Détails

Nous avons constaté qu'en février 2024, le Bureau du DGIFP avait élaboré un plan pour établir un calendrier et un plan d'action visant à moderniser les systèmes de TI essentiels à la mission afin d'atténuer les risques liés à la TI au niveau de chaque système. Nous avons examiné le plan de modernisation et constaté qu'il tient compte du soutien des applications, du soutien de l'infrastructure et de la probabilité de défaillance, et qu'il établit un plan d'investissement pour toute mise à niveau ou modernisation requise. Bien que ce plan, qui sera mis en œuvre d'ici mars 2025, aidera à atténuer les risques propres aux systèmes de TI, il ne devrait pas directement atténuer ou aider à cerner les risques de TI qui pourraient s'appliquer à l'échelle du groupe ou de la FPO, un problème relevé dans notre audit de 2022. Toutefois, ces risques propres au système de TI, une fois cernés et consolidés, serviront d'intrant pour cerner et atténuer les risques liés à la TI à l'échelle de la FPO.

Recommandation 2 : Mesure 3

- comparer périodiquement son registre des risques aux normes de l'industrie pour s'assurer que les risques énumérés sont pertinents et à jour.

État : En voie de mise en œuvre d'ici décembre 2024.

Détails

Nous avons constaté que le Bureau du DGIFP avait effectué une analyse du registre des risques actuels, qui consigne tous les risques opérationnels et de TI cernés par les ministères. Dans le cadre de cette analyse, le Bureau du DGIFP a constaté que plusieurs risques liés à la TI figurant

dans le registre des risques étaient incorrectement ou insuffisamment classés dans les catégories de risque opérationnel, car il n'y avait pas de catégorie distincte pour les risques liés à la TI. Il a également constaté que le risque lié à la TI n'a pas été suffisamment défini pour que la FPO puisse cerner, signaler et atténuer adéquatement les risques liés à la TI.

Le Bureau du DGIFP a utilisé un cadre de l'industrie reconnu à l'échelle mondiale, le cadre de gestion des risques de l'Association des professionnels de la vérification et du contrôle des systèmes d'information (ISACA), pour mettre en correspondance les risques de TI actuels dans le registre des risques avec quatre sous-catégories de risques de TI et fournir une méthodologie normalisée pour cerner, signaler et atténuer ces risques. Toutefois, le Bureau du DGIFP doit encore mobiliser le Bureau du chef de la gestion des risques pour communiquer cette nouvelle approche aux partenaires de TI de l'ensemble de la FPO et élaborer un plan d'action pour atténuer les risques actuels liés à la TI et cerner les nouveaux risques liés à la TI à l'aide du cadre ISACA, qu'il prévoit achever d'ici décembre 2024. Outre la mise à jour des catégories de risques liés à la TI, le Bureau du DGIFP n'a pas comparé son registre des risques liés à la TI actuels aux normes de l'industrie pour comparer et cerner les nouveaux risques liés à la TI.

3. Le centre de traitement de l'information le mieux coté de l'Ontario est considérablement sous-utilisé

Au cours du premier audit, nous avions constaté que le centre de données principal de l'Ontario n'était utilisé qu'à 30 %, même s'il a obtenu la cote la plus élevée disponible, ce qui indique que ses systèmes de TI sont en mesure de résister à tout type de défaillance. L'utilisation avait diminué au cours des cinq années précédentes, période au cours de laquelle une perte de 31 millions de dollars a été subie en coûts d'exploitation pour l'espace inoccupé, notamment pour les dépenses en électricité, en climatisation, en entretien et en sécurité physique.

Recommandation 3 : Mesure 1

Pour accroître l'utilisation du Centre de données de Guelph et renforcer ses contrôles existants d'accès des utilisateurs, le Bureau du directeur général de l'information pour la fonction publique devrait :

- déterminer le taux de recouvrement des coûts par pied carré ou par kWh pour ensuite effectuer une analyse coûts-avantages du taux de prélèvement le plus optimal afin d'attirer et d'intégrer plus d'entités gouvernementales;

État : En voie de mise en œuvre d'ici décembre 2024.

Détails

Nous avons constaté que le Bureau du DGIFP n'avait pas effectué d'analyse coûts-avantages, mais avait plutôt retenu les services d'Infrastructure Ontario en août 2023 pour évaluer l'utilisation du Centre de données de Guelph et proposer un futur modèle opérationnel. L'évaluation comprenait la rétroaction du secteur parapublic et des organismes de la Couronne, d'autres gouvernements provinciaux et d'entités du secteur privé. Les principales raisons invoquées dans l'évaluation de la faible utilisation sont l'utilisation accrue de solutions infonuagiques par le secteur parapublic et les organismes de la Couronne, le manque d'intérêt ou de besoin d'un centre de données de niveau IV et le coût supplémentaire associé à l'utilisation d'un centre de données. Au moment de notre audit de 2022, nous avions constaté que le centre de données de Guelph avait reçu la cote de niveau IV, soit la cote la plus élevée possible pour un centre de données, ce qui indique qu'il peut résister à tout type de défaillance.

L'évaluation d'Infrastructure Ontario a proposé trois options pour remédier à la faible utilisation. La première consistait à transformer le centre de données de Guelph de niveau IV en une installation de niveau III, ce qui réduirait le besoin et le coût d'une infrastructure supplémentaire pour l'entretien de l'installation, réduisant ainsi le taux de facturation pour l'utilisation du centre de données. Cela réduirait également les coûts d'intégration et d'utilisation des installations pour le secteur parapublic et les organismes de la Couronne. Une autre option proposée consistait à obliger légalement le secteur parapublic et les organismes de la Couronne le centre de données de Guelph. Toutefois, l'évaluation a révélé que de nombreux organismes du secteur parapublic et de la Couronne ont adopté des solutions infonuagiques ou ont exprimé le désir de maintenir leurs propres centres de données. La troisième option proposée consistait à vendre une partie du centre de données de Guelph et à conclure une entente hybride avec d'autres entités comme des municipalités. Le Bureau du DGIFP et le ministère des Services au public et aux entreprises et de l'Approvisionnement devraient prendre leur décision en fonction de ces options d'ici décembre 2024.

Recommandation 3 : Mesure 2

- évaluer s'il est faisable d'exiger que le secteur parapublic et les organismes de la Couronne transfèrent leurs activités au centre de traitement de l'information à leur taux de recouvrement des coûts;

État : Pleinement mise en œuvre.

Détails

Nous avons constaté que, dans le cadre de l'évaluation menée par Infrastructure Ontario, l'une des options envisagées était d'obliger légalement les entités du secteur parapublic (SP) et les entités de la Couronne ayant un mandat légal à transférer leurs activités de centre de données au centre

de données de Guelph. L'évaluation a révélé que, même si cela est techniquement faisable, il est peu probable qu'une mesure imposée soit approuvée par le Conseil du Trésor en raison de la faible demande et du coût élevé pour les entités du secteur parapublic (SP) et de la Couronne, ce qui en fait la moins privilégiée des trois options de la proposition. Infrastructure Ontario a fait appel à 33 organismes publics différents, y compris des organismes provinciaux comme le Conseil scolaire du district de Toronto, plusieurs universités et la Société des loteries et des jeux de l'Ontario. Selon les commentaires de ces organismes, la demande en solutions de stockage infonuagique s'accroît et la demande pour un centre de données de niveau IV est faible, voire nulle. On souligne également que de nombreuses entités du SP et de la Couronne ont adopté des solutions infonuagiques ou ont exprimé une volonté de maintenir leurs propres centres de données.

Recommandation 3 : Mesure 3

- mettre en œuvre une stratégie de sensibilisation auprès du secteur parapublic et des organismes provinciaux pour accroître l'adoption des centres de traitement de l'information;

État : En voie de mise en œuvre d'ici décembre 2024.

Détails

Nous avons constaté que la mise en œuvre de toute stratégie de sensibilisation potentielle à l'égard de l'utilisation du centre de données de Guelph dépend de l'option de l'évaluation d'Infrastructure Ontario choisie par le Bureau du DGIFP et le ministère des Services au public et aux entreprises et de l'Approvisionnement. Services technologiques d'infrastructure, une division du Bureau du DGIFP, avait élaboré en décembre 2023 une stratégie de colocation à mettre en œuvre si la décision de commercialiser le produit auprès des entités du secteur parapublic est retenue. La décision est attendue d'ici décembre 2024.

Recommandation 3 : Mesure 4

- examiner toutes les options proposées pour le futur modèle opérationnel du Centre de données de Guelph afin que la décision prise tienne dûment compte de l'économie et de la sécurité des données;

État : En voie de mise en œuvre d'ici mars 2025.

Détails

Nous avons constaté que l'évaluation effectuée en consultation avec Infrastructure Ontario était détaillée et comprenait des analyses des administrations dans plusieurs provinces et entités privées et publiques, et qu'elle tenait compte des coûts d'exploitation et des coûts facturés pour l'utilisation du centre de données. Le Bureau du DGIFP s'attend à ce qu'après un examen complet des options proposées, une option soit choisie d'ici décembre 2024, suivie de la préparation d'une analyse de rentabilisation qu'il soumettra à l'approbation du Conseil du Trésor d'ici mars 2025.

Recommandation 3 : Mesure 5

- Tout comme s'il s'agissait d'obtenir une attestation des membres de la FPO, le centre de traitement de l'information devrait établir un processus d'examen de l'accès des utilisateurs dans l'ensemble des organismes pour s'assurer que l'accès des utilisateurs au centre de traitement de l'information est supprimé dans les 24 heures suivant le licenciement de l'employé.

État : Pleinement mise en œuvre.

Détails

Nous avons constaté qu'en mai 2023, la division des Services technologiques d'infrastructure du Bureau du DGIFP a défini un processus d'attestation mensuel qui exige que tous les fournisseurs et les entités non membres de la fonction publique de l'Ontario (FPO) qui utilisent le centre de données de Guelph pour leurs activités de centre de données fournissent aux Services technologiques d'infrastructure une attestation selon laquelle ils ont été informés de tout changement dans leur situation d'emploi. Ce processus est mentionné dans le guide des politiques et procédures de contrôle de l'accès en matière de sécurité physique. De plus, une exigence a été ajoutée à la politique pour aviser la direction du centre de données de toute cessation d'emploi d'employés qui ne font pas partie de la FPO dans un délai de 24 heures. Nous avons constaté qu'une attestation a été remplie en août 2024 et stockée dans un dépôt indiquant que toute demande de retrait d'accès a été présentée.

4. La moitié de tous les systèmes de TI essentiels utilisés par la FPO n'ont pas de stratégie de reprise après sinistre

Lors de notre audit initial, nous avions constaté que près de la moitié (44 %) de tous les systèmes de TI qui sont essentiels à la continuité des services gouvernementaux n'avaient pas de stratégie de reprise après sinistre (RS).

Recommandation 4 : Mesure 1

Afin de réduire au minimum les interruptions des activités, le Bureau du directeur général de l'information pour la fonction publique devrait :

- collaborer avec les groupements de TI pour concevoir une stratégie de reprise après sinistre à l'échelle de la FPO et vérifier que tous les systèmes de TI essentiels ont établi et mis en place un plan de reprise après sinistre;

État : En voie de mise en œuvre d'ici mars 2025.

Détails

Nous avons constaté qu'en mars 2024, le Bureau du DGIFP a rédigé une stratégie détaillée de RS à l'échelle de la FPO. L'ébauche de stratégie propose plusieurs groupes de travail et comités qui tiendraient des réunions hebdomadaires, bimensuelles ou mensuelles afin de développer spécifiquement la capacité de récupérer les systèmes de TI actuels et d'établir la capacité de reprise après sinistre pour les systèmes hébergés dans le nuage en cas de catastrophe. De plus, la stratégie de reprise après sinistre définit les rôles et les responsabilités des groupements, des ministères et des Services technologiques d'infrastructure pour la conception, la mise en œuvre, la mise à l'essai et la reprise des systèmes. La stratégie a mis en correspondance chaque recommandation de notre Bureau portant sur les reprises après sinistre avec un plan d'action. Le Bureau du DGIFP est en train de faire approuver et mettre en œuvre la stratégie et le modèle de gouvernance proposé d'ici mars 2025.

Recommandation 4 : Mesures 2 et 3

- évaluer si tous les systèmes de TI nécessitent un plan de reprise après sinistre de façon continue;
- examiner et évaluer la conformité des groupements aux plans de reprise après sinistre au moins une fois par année et chaque fois qu'un changement important est apporté à l'environnement de TI de la FPO;

État : Peu ou pas de progrès.

Détails

Nous avons constaté que l'évaluation des systèmes de TI par le Bureau du DGIFP pour déterminer où un plan de reprise après sinistre est nécessaire constitue une étape ultérieure de la stratégie de reprise après sinistre à l'échelle de la FPO qui ne peut être lancée qu'une fois la stratégie approuvée

et mise en œuvre. Le Bureau du DGIFP est en train de créer un inventaire complet des systèmes de TI essentiels pour effectuer cette évaluation.

De même, un processus d'examen et d'évaluation de la conformité annuelle aux plans de reprise après sinistre ne peut être réalisé qu'une fois que le plan de reprise après sinistre a été approuvé et mis en œuvre.

Recommandation 4 : Mesure 4

- Tester périodiquement sa capacité à s'assurer que les systèmes de TI peuvent être rétablis en temps opportun dans un scénario catastrophe.

État : Peu ou pas de progrès.

Détails

Nous avons constaté que des essais périodiques des systèmes de TI pour assurer une reprise rapide devraient également être effectués dans le cadre des plans de reprise après sinistre qui n'ont pas encore été approuvés. Nous avons également remarqué que même si le groupement pour les services sociaux et les services à l'enfance et à la jeunesse (SSSEJ) et le groupement pour la justice ont effectué leurs propres évaluation de reprise après sinistre en 2023 sur un échantillon de systèmes de TI essentiels, cela a été fait de façon indépendante et n'a pas été intégré à la stratégie globale de reprise après sinistre.

5. La FPO ne dispose d'aucun fournisseur de réseau de secours pour assurer la continuité des opérations pour certaines activités essentielles

Lors de notre audit initial, nous avions constaté que le Bureau du DGIFP n'avait pas de fournisseur de réseau secondaire redondant pour certaines de ses activités essentielles, comme 44 centres de contact.

Recommandation 5 : Mesure 1

Pour assurer l'exploitation continue des systèmes de TI essentiels de la FPO, nous recommandons que le Bureau du directeur général de l'information pour la fonction publique :

- effectue une analyse coûts-avantages pour l'acquisition d'un fournisseur de réseau secondaire de secours pour ses activités essentielles;

État : Pleinement mise en œuvre.

Détails

Nous avons constaté que le Bureau du DGIFP avait effectué une analyse coûts-avantages dans trois secteurs d'activité différents afin de déterminer la nécessité d'un réseau secondaire de secours. Le Bureau du DGIFP a par la suite signé des contrats avec Bell pour le réseau de données de la FPO en janvier 2023 (accès Internet câblé et sans fil pour les ordinateurs de la FPO), ainsi qu'avec les centres d'appels des services vocaux et le réseau de mobilité (connectivité cellulaire pour les téléphones mobiles fournis par la FPO) en août 2023. Les ententes ont été mises en œuvre et Bell agit à titre de fournisseur de services de secours pour la FPO.

Recommandation 5 : Mesure 2

- modifier les contrats existants pour tous les fournisseurs afin d'inclure une clause de pénalité complète qui pourrait s'appliquer si les objectifs de rendement des ententes de niveau de service ne sont pas atteints.

État : En voie de mise en œuvre d'ici mars 2025.

Détails

Nous avons constaté que le Bureau du DGIFP avait inclus de nouvelles exigences obligatoires dans les contrats actuels pour la résilience du réseau, au lieu d'ajouter une clause de pénalité pour assurer la continuité des activités du gouvernement. Plus précisément, une exigence de redondance supplémentaire a été ajoutée, de sorte qu'en cas de défaillance d'une certaine partie du réseau, tout le trafic peut encore être desservi sur une autre partie du réseau. Cette exigence sera mise en œuvre d'ici mars 2025.

6. Les pratiques de cybersécurité de la FPO doivent être améliorées

Lors de notre audit initial, nous avons constaté que les données personnelles et sensibles n'étaient pas sécurisées de façon uniforme au moyen d'un chiffrement conforme à la norme de sécurité du Bureau du DGIFP. Nous avons également constaté qu'environ 11 000 des 40 000 employés de la FPO avaient suivi le cours obligatoire de sensibilisation à la cybersécurité en 2021. De plus, la formation de sensibilisation à la cybersécurité n'est pas requise pour environ 7 000 employés contractuels ni offerte chaque année à l'ensemble du personnel de la FPO, même si elle est considérée comme une pratique exemplaire.

Recommandation 6 : Mesures 1 et 2

Pour protéger les renseignements personnels confidentiels et sensibles des Ontariens contre toute divulgation non autorisée et accidentelle, le Bureau du directeur général de l'information pour la fonction publique devrait :

- faire appliquer aux groupements la norme de sécurité requise qui consiste à appliquer des contrôles de cybersécurité vigoureux comme le chiffrement;
- surveiller la conformité à la norme de sécurité exigeant le chiffrement des données sensibles.

État : En voie de mise en œuvre d'ici novembre 2025.

Détails

Nous avons constaté qu'en août 2023, le Bureau du DGIFP a collaboré avec le Bureau du directeur général de la gestion des risques (BDGGR), Politiques, Archives publiques et données, division du ministère des Services au public et aux entreprises et Approvisionnement, et le Bureau du conseiller provincial en matière de sécurité pour créer un cadre d'identification des actifs à valeur critique afin de déterminer les actifs de TI essentiels à la mission et aux activités, comme les systèmes de TI qui ont une incidence critique sur la FPO ou les Ontariens si les données sont compromises.

Nous avons examiné une ébauche du cadre d'identification des actifs à valeur critique , qui comprend un calendrier pour recenser les actifs à valeur critique à l'échelle de la FPO et les évaluer en fonction des menaces de cybersécurité. L'objectif du cadre, une fois les actifs recensés, est d'activer des mécanismes de protection, comme le chiffrement et la surveillance de la conformité aux exigences de chiffrement. Ce cadre était encore à l'état d'ébauche au moment de notre suivi, et les actifs à valeur critique n'avaient pas encore été identifiés afin d'appliquer des contrôles de cybersécurité robustes. Une fois le cadre élaboré, les actifs à valeur critique seront recensés afin

que des contrôles de sécurité comme le chiffrement puissent être appliqués. La mise en œuvre de ces contrôles de sécurité est prévue pour novembre 2025.

Recommandation 7 : Mesures 1 et 2

Pour réduire le risque d'erreur humaine dans le traitement de données sensibles et ainsi réduire l'exposition de la FPO aux menaces de cybersécurité, le Bureau du directeur général de l'information pour la fonction publique devrait :

- offrir des cours obligatoires de formation en cybersécurité à tout le personnel de la FPO, y compris les employés contractuels;
- examiner les rapports sur les taux d'achèvement des cours obligatoires et créer un processus de recours hiérarchique pour les cours obligatoires incomplets;

État : En voie de mise en œuvre d'ici mars 2025.

Détails

Nous avons constaté que l'accès à LearnON, la plateforme utilisée par la FPO pour offrir de la formation sur la cybersécurité, n'a pas été étendu aux employés contractuels, car ils ont besoin d'un numéro d'employé WIN de la FPO (numéro d'identification d'employé) pour accéder au réseau de TI de la FPO. Le Bureau du DGIFP a effectué une évaluation en mars 2023 et a noté qu'il n'est pas possible d'accorder au personnel qui n'est pas membre de la FPO l'accès à LearnON et a plutôt déterminé la nécessité d'un nouvel outil de formation dans ce but. Le SCT est en train d'acquérir un nouvel outil de formation qui permettra d'accorder l'accès aux employés contractuels et il le mettra en œuvre d'ici mars 2025.

Nous avons également constaté qu'afin de traiter les formations incomplètes et de les transmettre aux échelons supérieurs, le Bureau du DGIFP a établi des rapports réguliers sur l'achèvement des cours, et que les résultats ont été présentés au Conseil des cadres supérieurs de la technologie de l'information tous les trimestres. Nous avons examiné le rapport sur le cyberrenseignement de février 2024 et constaté que 44 % de tout le personnel de la FPO avait déjà suivi le cours obligatoire sur la classification de l'information.

Recommandation 7 : Mesure 3

- offrir une formation en cybersécurité à tout le personnel de la FPO au moins une fois par année;

État : En voie de mise en œuvre d'ici mars 2025.

Détails

Nous avons constaté que deux cours obligatoires sur la cybersécurité, la classification de l'information et les notions de base sur la cybersécurité, ont été élaborés et mis à la disposition de tout le personnel de la FPO par l'entremise de LearnON. Les cours ont été communiqués à tout le personnel de la FPO par courriel par le sous-ministre des Services au public et aux entreprises et de l'Approvisionnement, ainsi que dans le cadre d'une campagne annuelle de cybersécurité en octobre de chaque année afin de fournir des ressources supplémentaires sur les pratiques exemplaires en matière d'hameçonnage. Toutefois, à compter d'août 2024, ces cours ne doivent pas être suivis chaque année, mais seulement lorsque le personnel est intégré et quand tout changement important est apporté au cours. Le Bureau du DGIFP est en train d'étudier un mécanisme pour exiger que ces cours soient suivis chaque année et il les mettra en œuvre d'ici mars 2025.

Recommandation 7 : Mesure 4

- mettre en œuvre des contrôles de TI pour restreindre l'utilisation des appareils personnels afin d'empêcher les employés de la FPO qui travaillent à distance de stocker des données sur des appareils non liés à la FPO;

État : En voie de mise en œuvre d'ici décembre 2024.

Détails

Nous avons constaté que le Bureau du DGIFP avait mis en œuvre des contrôles par l'entremise de Microsoft 365 pour tous les appareils de la FPO afin d'empêcher le personnel de télécharger des fichiers sur des appareils personnels comme des clés USB ou des lecteurs externes. Cela se fait par l'entremise de Microsoft Intune, système informatique qui peut désactiver les ports USB des appareils afin que le périphérique de stockage amovible ne s'affiche pas pour les utilisateurs. Cette fonction est également utilisée pour empêcher les appareils non gérés ou non reconnus de télécharger et d'imprimer des documents. Le personnel peut demander une exemption à ce processus. Le Bureau du DGIFP examine actuellement la liste des exemptions pour en évaluer la pertinence. De plus, pour activer la fonctionnalité par l'entremise de Microsoft 365, certains employés doivent mettre leurs ordinateurs à niveau à Microsoft Windows 11. Les ordinateurs seront mis à jour vers Windows 11 en décembre 2024.

Recommandation 7 : Mesure 5

- appliquer une politique d'économiseur d'écran pour tous les utilisateurs.

État : Pleinement mise en œuvre.

Détails

Nous avons constaté que depuis le 1er avril 2024, tous les nouveaux appareils, comme les appareils informatiques et les ordinateurs portables des utilisateurs finaux, dans la FPO, sont déployés avec Windows 11 et que tous les appareils actuels ou en cours d'utilisation passeront de Windows 10 à 11 en fonction de leur cycle d'actualisation. Nous avons examiné les paramètres globaux de Windows et constaté que tous les appareils Windows 10 et 11 ont été configurés de manière à respecter une limite d'inactivité de 15 minutes avant que les écrans soient verrouillés et qu'un mot de passe soit requis. Cela devrait accroître la conformité à la politique d'économiseur d'écran automatique obligatoire de la FPO. Toute exemption à la présente politique et au paramètre d'économiseur d'écran Windows connexe exigera que le personnel remplisse un formulaire de report du traitement des risques qui nécessite l'approbation de ses secteurs de programme et de la TI.

Recommandation 8 : Mesure 1

Pour contribuer à la lutte contre les cyberattaques et accroître la mobilisation à l'égard des pratiques exemplaires de prévention pour les entités du secteur parapublic confrontées à de telles cyberattaques, le Bureau du directeur général de l'information pour la fonction publique devrait établir un protocole d'entente avec le secteur parapublic pour partager des rapports détaillés sur les incidents de cybersécurité et communiquer au sujet des moyens de remédier aux faiblesses.

État : En voie de mise en œuvre d'ici novembre 2025.

Détails

Nous avons constaté que le Bureau du DGIFP avait collaboré avec le SCT pour inclure des dispositions sur la cybersécurité dans les modifications mises à jour proposées pour le modèle de protocole d'entente entre les ministères et les organismes du secteur parapublic, et pour les utiliser dans tout nouveau protocole d'entente. Plus précisément, le Bureau du DGIFP a proposé une exigence obligatoire mettant en place un rôle spécialisé au sein des ministères ou des organismes du SP responsable de la formation et de la sensibilisation des employés aux pratiques exemplaires en matière de cybersécurité. De plus, les modifications proposées comprennent l'établissement et l'exécution d'un programme global de cybersécurité et le signalement des cyberincidents critiques au conseil d'administration de l'organisme et à la division de la cybersécurité du Bureau du DGIFP. Des inclusions sont également proposées pour la documentation des risques liés à la TI, des évaluations fréquentes de la cybersécurité et la présentation de rapports trimestriels de toute menace liée à la TI au Bureau du DGIFP. Le modèle de protocole d'entente mis à jour devrait être mis en œuvre d'ici novembre 2025.

Recommandation 9 : Mesures 1, 2 et 3

Pour déterminer les risques auxquels les données du gouvernement de l'Ontario peuvent être exposées, le Bureau du directeur général de l'information pour la fonction publique devrait :

- établir un processus centralisé pour exiger la réception et l'examen des rapports d'assurance de tiers des fournisseurs qui hébergent ou utilisent les données de la FPO;
- examiner les lacunes en matière de TI relevées dans les rapports d'assurance de tiers pour en évaluer l'incidence sur les opérations de la FPO et prendre des mesures correctives au besoin;
- collaborer avec les groupements de TI pour désigner les fournisseurs qui stockent des données à l'extérieur du Canada, évaluer les risques et prendre des mesures correctives si le stockage contrevient aux exigences relatives à la collecte, à la conservation et à l'élimination des renseignements de nature délicate associés au stockage des données à l'extérieur de l'Ontario.

État : En voie de mise en œuvre d'ici octobre 2025.

Détails

Nous avons constaté que le Bureau du DGIFP avait mis sur pied un bureau provisoire de gestion des fournisseurs de TI. La responsabilité de ce bureau consiste à superviser et à surveiller les fournisseurs de TI tiers et les risques connexes. Les groupements de TI seront chargés de recevoir et d'examiner les rapports d'assurance des contrôles du système et de l'organisation de tiers afin de repérer les exceptions, de les traiter directement avec les fournisseurs et de communiquer les résultats au Bureau de gestion des fournisseurs de TI. De plus, les groupements de TI sont maintenant responsables de cibler les fournisseurs qui stockent des données à l'extérieur du Canada, d'évaluer les risques liés à la résidence des données et, au besoin, de prendre des mesures correctives. En outre, les groupements de TI et les ministères peuvent maintenant communiquer directement avec la Division de la cybersécurité par l'entremise d'un nouveau service à l'échelle de la FPO, le Cyber Procurement Advice, qui a été déployé en septembre 2023 pour recevoir des directives sur la façon d'évaluer et de gérer les risques liés à la résidence des données. Le mandat du Bureau de gestion des fournisseurs de TI a été inclus dans la politique de gestion des risques de cybersécurité, approuvée en avril 2023. Jusqu'à ce qu'un bureau de gestion des fournisseurs de TI attitré soit établi (prévu en octobre 2025), le Bureau du DGIFP a mis en place un processus pilote pour les groupements de TI afin d'examiner les rapports d'assurance des CSO des cinq principaux fournisseurs en fonction des dépenses du Bureau du DGIFP. Le Bureau provisoire de gestion des fournisseurs examinera les constatations rapportées par les groupements de TI et les plans d'atténuation proposés pour déterminer si une formation supplémentaire sur les rapports des CSO pour les groupements est nécessaire.

7. L'inventaire des systèmes de TI du gouvernement de l'Ontario est incomplet et inexact

Lors de notre audit initial, nous avions constaté que l'inventaire des systèmes de TI ne contenait pas tous les renseignements pertinents et essentiels sur chaque système de TI. De plus, nous avions constaté que le processus actuellement en place pour examiner l'inventaire ne prévoyait pas d'examens rigoureux, réguliers et uniformes fondés sur des critères afin de vérifier que l'information stockée est exacte, complète et à jour.

Recommandation 10 : Mesures 1, 2 et 3

Pour améliorer l'exactitude et l'exhaustivité de l'inventaire des systèmes de TI et pour repérer plus facilement les systèmes de TI vieillissants, le Bureau du directeur général de l'information pour la fonction publique devrait :

- élaborer pour tous les employés des lignes directrices décrivant un processus de mise à jour de la base de données de gestion de la configuration à l'aide d'un ensemble défini de critères;
- remplir tous les champs obligatoires vides dans la base de données de gestion des configurations;
- procéder à un examen systématique de la base de données tous les ans et chaque fois qu'un système est intégré ou mis hors service.

État : ◉ Pleinement mise en œuvre.

Détails

Nous avons constaté qu'en juin 2023, le Bureau du DGIFP a mis sur pied des séances de formation sur la base de données de gestion de la configuration (BDGC), qui décrivent en détail la façon dont les actifs sont gérés au sein de la BDGC et les données nécessaires requises. La formation a été offerte aux responsables des éléments de configuration, c'est-à-dire aux personnes responsables de maintenir l'exactitude de l'information dans la BDGC pour un système de TI particulier. La formation précise les champs de saisie de données disponibles dans la BDGC et les données qui devraient y être fournies, ainsi que les scénarios ou erreurs courants qui peuvent être rencontrés dans la BDGC et les renseignements supplémentaires nécessaires.

Nous avons constaté que le Bureau du DGIFP avait mis sur pied des réunions bimensuelles pour examiner la qualité globale des données dans la BDGC au moyen d'un rapport sur la qualité des données qui peut être généré à partir d'un tableau de bord PowerBI et qui indique des champs incorrects, périmés ou vides. Nous avons examiné les rapports sur la qualité des données en mars

et juillet 2024 et constaté que le nombre de champs vides a considérablement diminué et que la qualité globale des données s'est améliorée depuis notre audit de 2022. On ne s'attend pas à ce que les champs soient remplis à 100 %, car il existe toujours une marge d'erreur raisonnable. Les réunions bimensuelles visant à examiner la qualité des données sont exhaustives et comprendraient tout système de TI qui a été intégré ou mis hors service de façon continue.

Recommandation 11 : Mesures 1, 2 et 3

Pour assurer un processus vigoureux de gestion des licences de logiciels et éviter les paiements insuffisants ou les trop-payés aux fournisseurs, le Bureau du directeur général de l'information pour la fonction publique devrait :

- intégrer ses principaux systèmes de TI à son système logiciel de gestion des actifs afin qu'il puisse suivre l'utilisation et évaluer l'usage optimal et économique des ressources;
- adopter un processus de vérification et de confirmation que les licences en main correspondent aux frais payés aux fournisseurs;
- effectuer des vérifications régulières des logiciels installés pour déterminer la nécessité d'acheter ou de retirer des licences de logiciels.

État : En voie de mise en œuvre d'ici juin 2025.

Détails

Nous avons constaté qu'en janvier 2024, le Bureau du DGIFP a signé un contrat avec un fournisseur pour gérer le processus de gestion des licences logicielles de la FPO. Le fournisseur a fixé au mois de juin 2025 le calendrier d'intégration des logiciels existants à Snow, l'outil de gestion des licences logicielles de la FPO, ainsi que l'élaboration d'un processus de rapprochement des licences logicielles avec les frais payés et de vérification des logiciels installés.

8. Diligence raisonnable insuffisante lors de l'embauche de consultants en TI

Au cours de notre audit initial, nous avions constaté que le Bureau du DGIFP n'effectuait pas d'évaluations internes de la capacité pour déterminer si un consultant en TI était requis avant d'en embaucher un. Nous avons également constaté que les conseillers en TI avaient reçu une rémunération supérieure au taux recommandé indiqué dans le manuel des services de placement des employés de la FPO, sans justification. Nous avons également constaté qu'il n'y avait aucune exigence quant au nombre minimal de candidats à interviewer pour chaque poste ou au nombre d'évaluateurs en entrevue.

Recommandation 12 : Mesures 1, 2, 3 et 4

Pour veiller à ce que les consultants fassent preuve de diligence raisonnable et pour optimiser les ressources, le Bureau du directeur général de l'information pour la fonction publique devrait :

- veiller à ce que des analyses coûts-avantages soient effectuées lors de l'acquisition de services supplémentaires et à ce que l'option d'embaucher un employé à temps plein soit envisagée;
- rémunérer les consultants selon les échelles de taux recommandées qui sont énoncées dans le manuel des services de placement des employés et veiller à ce que toute dérogation ou exception au manuel soit formellement documentée et approuvée par le Bureau du directeur général de l'information pour la fonction publique;
- s'assurer qu'au moins deux candidats par poste sont interviewés par au moins trois évaluateurs;
- documenter officiellement et conserver les notes d'entrevue dans le système de TI.

État : Pleinement mise en œuvre.

Détails

Nous avons constaté que le Bureau du DGIFP collabore avec Gestion de la chaîne d'approvisionnement Ontario (GCAO) pour mettre en œuvre un modèle d'analyse coûts-avantages fondé sur l'exigence initialement énoncée dans la directive sur l'approvisionnement pour la FPO depuis 2018. De plus, le Bureau du DGIFP a mis à jour le Système de gestion de l'information sur les fournisseurs (SGIF) en août 2023 pour y inclure une attestation obligatoire indiquant que le ministère ou le groupement a réalisé l'analyse coûts-avantages dans le cadre du processus d'approbation d'un approvisionnement particulier. Les gestionnaires qui remplissent un formulaire d'approvisionnement dans le SGIF ne peuvent le remplir jusqu'à ce que l'attestation soit terminée. Un bulletin officiel de ces changements a été envoyé au personnel du Groupement pour les organismes centraux en octobre 2023. Le groupement pour les organismes centraux effectue également des vérifications ponctuelles trimestrielles pour s'assurer de la conformité à la Directive sur l'approvisionnement et au Manuel des services de placement des employés et, à compter d'août 2023, a inclus un nouvel élément pour vérifier si des analyses coûts-avantages ont été effectuées. En juillet 2024, le groupement pour les organismes centraux n'a relevé aucune non-conformité à l'exigence d'analyse coûts-avantages.

Nous avons également remarqué que le Bureau du DGIFP a mis à jour la configuration de l'outil du SGIF afin d'éviter qu'un taux de rémunération qui ne correspond pas à la fourchette recommandée du manuel du service de placement des employés de la FPO soit saisi dans l'outil sans sélectionner

un nouveau champ indiquant qu'une exception a été approuvée par le Bureau du DGIFP. L'outil SGIF exige également qu'une raison supplémentaire soit sélectionnée dans un menu déroulant pour expliquer pourquoi l'exception a été faite, comme des ensembles de compétences spécialisées.

Nous avons constaté que le Bureau du DGIFP a envoyé un bulletin sur les pratiques exemplaires en juillet 2023 à tous les gestionnaires recruteurs soulignant l'exigence d'au moins deux candidats et d'au moins trois évaluateurs pour chaque poste de consultant en TI. Une attestation a également été ajoutée au SGIF pour indiquer que ces exigences ont été respectées et que les notes d'entrevue ont été téléversées dans le SGIF. Les notes d'entrevue et les attestations téléchargées ont également été ajoutées à la vérification ponctuelle trimestrielle effectuée par le groupement pour les organismes centraux.

Recommandation 13 : Mesures 1, 2 et 3

Pour rétablir efficacement les services de TI avec un minimum d'interruption pour les Ontariens, calculer avec exactitude la conformité aux objectifs de prestation des services et en rendre compte, le Bureau du directeur général de l'information pour la fonction publique devrait :

- réévaluer ses cibles de conformité pour s'assurer qu'elles correspondent aux normes de l'industrie;
- examiner le calcul du temps de résolution des incidents pour s'assurer qu'il est conforme aux pratiques exemplaires de l'industrie;
- mettre en place des mesures correctives pour améliorer le délai de rétablissement des services de TI.

État : ◉ Pleinement mise en œuvre.

Détails

Nous avons constaté que le Bureau du DGIFP avait collaboré à une analyse exhaustive des ententes sur les niveaux de service avec Gartner, une société de recherche en TI de premier plan au sein de l'industrie, et conclu, sur la base des résultats de l'analyse, que ses cibles de conformité étaient conformes aux pratiques exemplaires de l'industrie et aux exigences existantes de la FPO. Le Bureau du DGIFP nous a informés qu'il suit les pratiques exemplaires indiquées dans la documentation fournie avec son logiciel de gestion des services de TI. De plus, le Bureau du DGIFP a comparé sa méthode de calcul à celle utilisée avec d'autres outils de gestion des services similaires et a jugé que ses échéanciers de résolution des incidents de TI étaient adéquats ou conformes aux normes de l'industrie. Nous avons également constaté que le Bureau du DGIFP effectue des analyses des données historiques et actuelles sur le rendement afin de cerner les

lacunes à améliorer, en particulier en ce qui concerne l'amélioration du temps de résolution des incidents par les fournisseurs de services de TI.

Recommandation 14 : Mesures 1 et 2

État : Pleinement mise en œuvre.

Détails

En raison de la nature délicate de la cybersécurité et afin de réduire au minimum le risque d'exposition pour la FPO, les détails pertinents de cette constatation et de cette recommandation n'ont pas été publiés dans notre audit de 2022 et ont plutôt été fournis directement au Bureau du DGIFP aux fins de correction. Le Bureau du DGIFP s'est engagé à donner suite à ces constatations en temps opportun, et nous ferons le suivi de l'état de cette recommandation directement auprès du Bureau du DGIFP. L'état détaillé de cette recommandation ne sera pas publié dans le rapport de suivi.

Recommandation 14 : Mesure 3

État : En voie de mise en œuvre d'ici mars 2025.

Détails

En raison de la nature délicate de la cybersécurité et afin de réduire au minimum le risque d'exposition pour la FPO, les détails pertinents de cette constatation et de cette recommandation n'ont pas été publiés dans notre audit de 2022 et ont plutôt été fournis directement au Bureau du DGIFP aux fins de correction. Le Bureau du DGIFP s'est engagé à donner suite à ces constatations en temps opportun, et nous ferons le suivi de l'état de cette recommandation directement auprès du Bureau du DGIFP. L'état détaillé de cette recommandation ne sera pas publié dans le rapport de suivi.

// Annexe

Aperçu de l'état des mesures recommandées

	Nombre de mesures recommandées	Pleinement mise en œuvre	En voie de mise en œuvre	Peu ou pas de progrès	Ne sera pas mise en œuvre	Ne s'applique plus
Recommandation 1	2		2			
Recommandation 2	3		3			
Recommandation 3	5	2	3			
Recommandation 4	4		1	3		
Recommandation 5	2	1	1			
Recommandation 6	2		2			
Recommandation 7	5	1	4			
Recommandation 8	1		1			
Recommandation 9	3		3			
Recommandation 10	3	3				
Recommandation 11	3		3			
Recommandation 12	4	4				
Recommandation 13	3	3				
Recommandation 14	3	2	1			
Total	**43**	**16**	**24**	**3**	**0**	**0**
%	100	37	56	7	0	0